University of Texas School of Law

Cybersecurity Law and Policy

Prof. Bobby Chesney

(FALL 2018)

Top-Level Overview

I. THE DEFENSIVE PERSPECTIVE

A. Punishing Unauthorized Access: Imposing Costs on Attackers

1. August 29 Introduction: Attack, Black Markets, and Crime

2. August 30 Introduction: Vulns, Exploits, Disclosure, and Patching

3. September 5 Prosecution: When is hacking criminal?

4. September 6 Prosecution: Other criminal statutes

5. September 12 Criminal liability concluded; Civil liability introduced

6. September 19 What if the attacker is a foreign government? (I)

7. September 20 What if the attacker is a foreign government? (II)

8. September 26 What if the attacker is a foreign government? (III)

9. October 3 What if the attacker is a foreign government? (IV)

B. Encouraging Potential Victims to Better Protect Their Systems

10. October 4 The Role of Regulators: Rulemaking & Enforcement

11. October 10 *Last class continued*

12. October 11 The Role of Private Lawsuits and Insurance

13. October 17 Pruning Disincentives and Leveraging Purchasing Power

14. October 18 *Last class continued*

15. October 24 Getting the Government to Protect Itself Better

16. October 25 *Last class continued*

C. After the Fail: Consequence Management

17. October 31 Cases of National Significance

18. November 1 *Last class continued*

II. THE OFFENSIVE PERSPECTIVE

19. November 7 Should We Allow the Private Sector to Hack Back?

20. November 8 Hacker cops? Network Investigative Techniques

21. November 15 *Last class continued*

22. November 28 Spy games: Hacking as Espionage & Covert Action

23. November 29 Cyber War? Introduction to Cybercom
24. December 5 Cyber War? International Law Concerns

III. CRISIS SIMULATION

25. December 6 Crisis Simulation

FINAL EXAM

December 14

Readings and Questions

I. THE DEFENSIVE PERSPECTIVE

For the first half of the course, we will focus on the *defensive* perspective. That is, we will focus on the overarching public-policy goals of (i) minimizing unauthorized access to (or disruption of) computers and (ii) mitigating harm when such access or disruption occurs.

When it comes to minimizing unauthorized access and disruption, the main idea is to increase both the undesirable consequences attackers risk and the level of difficulty they face if they are not deterred. There is a lot of room for improvement on both dimensions, no doubt; plenty of targets are not difficult to access or disrupt, and attackers often stand to gain much more than they realistically stand to lose.

Our goal is to understand the various institutions, policies, and legal frameworks that define the status quo on these matters; to grasp the competing interests that are in play; and to wrestle with the question of how we might do better.

We will subdivide the defensive unit in a way that tracks these considerations. First, we will spend several classes examining the current U.S. approach to impose consequences on attackers (including criminal and civil forms of liability, but also non-legal modes of punishment). Second, we will several more classes examining forces that, by design, incentivize potential victims to do more in their own defense (or, more to the point in many cases, in defense of their customers, employees, etc.). And then we will conclude with a sequence examining what happens when attackers nonetheless succeed, looking at consequence management both in "normal" cases and those that have national significance.

A. Punishing Unauthorized Access: Imposing Costs on Attackers

A note on terminology up front: we will often use the word "attacker" as a shorthand referring to a person or organization that seeks to access a system in an unauthorized way (or to disrupt the proper functioning of a system).

Attackers come in many shapes and sizes. Some are sophisticated professionals, others are rank amateurs. Some are state-sponsored, some are part of non-state organized groups, and some are individuals. Some are crooks. Some are spies (including *our* spies; spies isn't pejorative). Some are just showing off skills. Some are in it for the laughs. Some do it to settle personal scores. Some are seeking competitive advantage. Some mean well, hoping to spur people to try harder on defense by exposing weaknesses in hopes that they'll be remedied. Some are malicious, hoping to cause harm (or to use your system to cause harm to others). The point being: there are *many* potential attackers out there, with a wide variety of motives and capacities, some awful and others laudable. Bear this in mind as we examine the various tools that we currently have—or might one day have—to impose consequences on attackers.

We start this sequence with a warm-up class, familiarizing ourselves with terms and contexts relating to the criminal side of our topic. Class 1 explores the black markets in which various things of value relating to cybersecurity—stolen data, access to control compromised machines, tools to breach systems—are bought and sold. After that, we have a pair of classes focused on the federal law enforcement entities that are relevant for cybersecurity and the federal criminal laws (especially the Computer Fraud and Abuse Act, aka "CFAA") they enforce. The CFAA is not really just one law, but several distinct ones. It raises fascinating and difficult questions of interpretation and design. We will dive deep into the CFAA as it has been used in practice, examining several controversial prosecutions and key

current issues. We also will look at other federal laws that attacks may implicate, and we will note that there are similar (but sometimes conspicuously-different) provisions found in state law (not to mention the laws of foreign states).

In Class 4, we will turn our attention to a different type of cost that might be imposed on an attacker: civil liability (especially damages). The CFAA has a role to play here too, but we'll also take note of several other sources of potential liability. We will pay particular attention to the reasons it may be hard to make effective use of this tool, and we will consider whether and why changes to the legal architecture might make sense.

Next, we will turn in Classes 5 and 6 to consider a special breed of attacker: states. States sometimes attack using their own government-employed personnel, and they sometimes outsource the function to private, semi-private, and faux-private actors (see the writings of Tim Maurer on this). At any rate, the phenomenon of state-sponsored attacks raises a host of complex policy questions. We will first spend time considering concepts like attribution, deterrence, cross-domain deterrence, and escalation, and then we will look at a series of recent case studies (involving Russian and Chinese attacks on US entities) in order to understand which tools do and do not seem to have bite in this distinct setting.

1. August 29 – Introduction: Attack, Black Markets, and Crime

- **Start by generating a long list of reasons (stated at a high level of generality) why someone might try to gain unauthorized access to (or disrupt the functioning of) a computer or network.** Bear in mind that some attackers are private individuals, while others may be part of larger organizations (private or governmental). Perhaps make separate lists?
- When a person or entity wants to gain unauthorized access to (or disrupt the functioning of) a computer or network, it certainly helps if that person or entity already has the skill and resources needed to develop tools to suit that purpose. But not everyone does, and in any event it is not necessary in all cases. Why not? Because there is a thriving black market for the sale not only of stolen information, but also the sale of the means to steal and disrupt. ***Read chapters 2-4 of this 2014 RAND study*** to learn more, and then consider the questions below.
- **Who participates in these black markets, and has the answer to that question changed over time?** Note factors such as nationality, and expertise. **What are the policy implications of your answers?**
- **Can you explain how the types of products/services sold on the black market have changed over time as well, and why this matters from a policy perspective?**
- **What are botnets, and how has their use evolved over time?**
- People often mention the botnet problem in connection with the growth of IoT (that is, the "Internet of Things," which is a shorthand for the growing constellation of household and personal devices with Internet connectivity of some kind). **Why might that be?**
- Obviously, anonymity is important to participants in the cybercrime black markets. ***Read this January 2017 Wired article from Andy Greenberg*** for an introduction to how these markets and their participants try to remain hidden. **Be prepared to explain what terms like "deep web," "dark web," and "TOR" signify.**
- **Which policy arguments might favor allowing at least some such hidden services to exist? Which favor suppressing them? How should these interests be reconciled? Should the balance should be the same in all societies? Why might that be hard in practice?**
- Sometimes government does succeed in "taking down" a particular dark web market. The RAND report suggests such successes are "transitory," however. **Why? What follows from this?**

2. August 30 - Introduction: Vulns, Exploits, Disclosure, and Patching; Crime

A. More introductory concepts

- *Note: In class we had an extensive discussion about the meaning of "vulnerability," "exploit," "disclosure," "patching," and related concepts. The original syllabus did not have specific readings, let alone question prompts, about this. But we spent most of class #2 on those introductory matters.*
- Refer to the RAND study above. **What are "zero-day vulnerabilities" and what is special about them?**

B. Who are the law enforcement players?

- **What is the office at DOJ that has special responsibility for this area? *Read this*.**

- **What about the FBI? *Read this for a general overview*.**
- **What is the role of the U.S. Secret Service, and why is it involved? *Read this to understand the Secret Service's role.***
- We are focused for the moment on prosecuting hacking as a crime. But it's worth pausing to reminder ourselves that "crime" is not always the most relevant category, even if a given hack is a crime. So stretch your mind a bit: **When DOJ decides to prosecute, how might this have implications—perhaps negative ones?—for the missions of other government agencies or departments?**

3. Sep. 5 - Prosecution: When is hacking criminal?

Note: During this class we spent all our time reviewing and parsing the language of the CFAA, and did not reach the case studies. The case studies were therefore pushed off to class #4. I have now adjusted this version of the syllabus to list the case studies under class #4, instead of here in class #3.

A. Introduction to the Computer Fraud and Abuse Act ("CFAA")

- There are *many* federal crimes that might be implicated by the activity we are discussing, but the most significant one is the Computer Fraud and Abuse Act, or CFAA. The CFAA is codified in Title 18 of the United States Code (the U.S. Code is the compilation of federal statutes organized topically, and Title 18 is the main place to find federal criminal laws). In particular, it is codified as 18 U.S.C. Section 1030. In a moment I want you to read key parts of it. For some of you, this will be your first time to really examine a criminal statute. You may be surprised how convoluted it seems to be! Alas…you'll get used to it. Now, on to business. Anyway, here's how I want you to do it. ***Click here and read—very slowly—the first subsection (1030(a)).*** As you will see, subsection 1030(a) contains *seven separate* criminal offenses. Let that sink in. CFAA is not one criminal prohibition, but *seven*. Each one could be a stand-alone section. But they aren't, and we just have to deal with that. You can handle it!
- Now that you've had a chance to skim all of 1030(a), it's time to go back and really understand what makes those seven provisions different from one another. We will spend loads of time in class on this, so take it seriously! **Try making a chart that has the number of each subsection, some sort of pithy label or name that helps you remember what a particular subsection is focused on, and then a bullet-point list of the "elements" that appear to be necessary in order to be guilty of an offense under that subsection.** On the elements, be sure to ask yourself: **What action(s) are necessary? What mental state seems required? Any other necessary conditions? And how is this different from the others?**
- For each of the seven provisions: **Can you articulate the policy argument in favor of making each scenario a crime? Counterarguments?**
- Notice that the CFAA goes on, in subsection 1030(b), to include a clause creating liability for conspiracies and attempts to commit those offenses. **Can you articulate pros and cons?**

4. September 6 – Prosecution: Other criminal statutes

Note: In class we spent a great deal of time on a hypothetical scenario at the start of class, and then proceeded to cover the Morris case study and part of the Nosal case study. As a result, we will use class #5 in part to cover the remainder of the Nosal case study, the Swartz case study, and the material on the Wire Fraud statute and other items involving

other criminal laws listed here in class #4. And for that reason, I've now adjusted the listing of readings and questions for class #4 to simply refer to the case studies, pushing the rest of the material over to class #5.

A. Case Studies of the CFAA in Practice

- The first big CFAA prosecution involved the ground-breaking—and largely accidental — "Morris Worm." **Read about the underlying events here**, and then **read the court opinion affirming his conviction here** (*United States v. Morris*, 928 F.2d 504 (2d Cir. 1991)).
- **Do you agree that Morris violated the CFAA? Can you make the argument that this prosecution was desirable? Can you make the opposite argument? Which view is most persuasive to you? Would you alter the CFAA to produce a different result?**
- The controversy surrounding the Morris case was nothing compared to that generated by the prosecution of Aaron Swartz. **Read about that here,** and then **consider the same questions as above.**
- Another much-discussed example concerned David Nosal, who once worked for the executive search-and-recruitment firm Korn/Ferry and then left to start a competitor. Then things got interesting. **Read about the CFAA charges in his case, the issues they raised, and the outcome as explained by the "en banc" Ninth Circuit Court of Appeals in *United States v. Nosal***, 676 F.3d 854 (2012). **Be prepared to explain the government's theory of how the CFAA was violated (including which subsection), Nosal's counterargument, and how the court resolved things—and don't forget to decide which side you would take and why.**
- The government on remand re-tried Nosal on a different theory: **read here** to see what happened next. **What was the revised theory, and what do you think of it?**

5. September 12 – Criminal liability concluded; Civil Liability introduced

Note: Because we proceeded slowly in earlier classes, class #5 actually will begin with a brief discussion of the second-half of the Nosal case study and also the Aaron Swartz case (holdover material from the last class).

A. Other Relevant Criminal Laws

- CFAA isn't the only tool in the toolbox for federal prosecutors dealing with cyber crime. There are some statutes of more-general applicability that often fit well with hacking scenarios, and there also are some highly-tailored statutes to consider. The most-relevant of the generally-applicable criminal laws, in this respect, is the "wire fraud" statute**. *Read 18 USC 1343***. **How does it differ from CFAA? Can you explain why a prosecutor might find it handy?** To get a further sense of what a wire fraud prosecution linked to hacking might look like, **check out this article** about an unusual wire fraud prosecution. Gooooooooooooooooooal!
- Apart from "wire fraud," there are several other, more-specific fraud statutes. While I do not intend for you to learn the particulars with them (as you will with CFAA and wire fraud), I do want you to be familiar with the general idea behind them. So: **skim the following sufficiently to be able to articulate what they forbid: 18 USC 1028** (identity fraud), **18 USC 1028A** (identity theft), and **18 USC 1029** ("access device" fraud). **Be sure to be able to explain what an "access device" is!**

- For a fascinating case showing how a variety of these statutes might be used in combination, we will discuss the prosecution of Roman Zeleznev (aka "Track2"). ***Read about it here***. This case turned out well for the government; do you think it indicates that similar success is possible in most such cases? Read this and this for a glimpse of some unusual complications. **What made this case harder than normal? What factors explain how DOJ prevailed anyway? Does this show DOJ can generally prevail in similar cases?**
- Note: There are other criminal laws that are important in this space, but that we will not explore them in the interests of moving along to other topics. For the record, however, I'll still proceed to name a few of them: 18 USC 641 (theft of government property); 18 USC 2511 (unauthorized interception of communications); 18 USC 2701 (unauthorized accessing of stored communications); and 18 USC 793-798 (various provisions relating to espionage and protection of defense information). There also is 17 USC 1201-1205, aka the Digital Millennium Copyright Act ("DMCA"). We will study the DMCA in more detail in a later class).

B. State Criminal Laws

- States have statutes analogous to the CFAA. For an overview of the relevant Texas statute, including observations on how it differs from CFAA in certain respects, ***read this***. **Can you articulate whether/how this differs from the CFAA?** For a sense of the state agency responsible for computer crime investigations, by the way, **read *here***.

C. International cyber crime enforcement

- The United States is party to the "Budapest Convention on Cybercrime." ***Skim its provisions*** to get a rough sense of what it is trying to accomplish. **What do the parties to this treaties actually promise to do that seems genuinely significant? Why do you suppose Russia, China, and Iran are not parties to this treaty?**

D. CFAA as a basis for civil suit

- Well, it turns out the CFAA is not just a *criminal* statute, but also a *civil liability* statute (that is, it also creates a "private right of action" enabling suits for money damages in certain circumstances). ***Read 10 U.S.C. Section 1030(g).*** For such a short subsection, there is a LOT going on here!
- First, there is a complicated precondition for exercising that right to sue, to the effect that only certain conduct counts. **Can you unpack the statutory cross-references and explain, in plain English, when someone is allowed to sue? Can you explain what this leaves out, and why Congress might have gone to such trouble to draw this line? Do you agree with this approach?**
- Next, there's a sentence that limits the plaintiff to "economic damages" for a certain type of case. **What does this mean, what type of case counts, and what explains all this?**
- We'll skip over the statute of limitations (that is, the part that says you only get two years to sue). That brings us to the last sentence of 1030(g). **What precisely does this last sentence do? Be prepared to make both pro and con arguments for this provision.**

E. CFAA Civil Suit Case Studies

- Social media companies like Facebook and LinkedIn at times turn to the CFAA (using its civil liability provisions) in an effort to stop other companies from collecting information from public-facing parts of their sites. Whether and when such conduct violates the CFAA is a hot current issue. ***Read about the suit Facebook filed against "Power Ventures" here and here*. Be able to describe how Power Ventures made use of data found on Facebook pages, why Facebook claimed this violated the CFAA, why Power Ventures took the contrary view, and how the courts resolved the matter** (note: The Supreme Court recently refused to review the appellate court's ruling, ending the case).

- *HiQ v. LinkedIn* is a similar, recent case. ***Read about it here and here*. Same questions as to the Power Ventures clash with Facebook. What are the larger policy stakes?** (The litigation in this one continues, with the Ninth Circuit Court of Appeals having heard oral argument last spring and the resulting decision not yet having issued).

No class on September 13 (makeup TBD)

6. September 19 What if the attacker is a foreign government? (I)

A. Key concepts

- Up until now, we have proceeded from the assumption that instances of unauthorized access involved run-of-the-mill criminal or tortious activity conducted by private individuals or organizations. But sometimes the perpetrator is acting on behalf of a foreign government. Governments hack for many different (and sometimes overlapping) reasons, and we need to introduce these possibilities before turning to the questions that arise when we consider how the U.S. government attempts to impose costs on foreign governments in these situations. The primary reasons, in no particular order, include:

    - ***Law Enforcement:*** A government may engage in hacking to advance its own law enforcement interests (hacking to investigate or gather evidence, or perhaps even to do something to set up an arrest or other action).

    - ***Crime:*** Some regimes are desperate for cash. Private persons are not the only ones who might hack for financial gain.

    - ***Information Collection***: Most states are in the business of stealing secrets in order to inform decisionmaking or to advance other goals, though states vary widely in their capacity to actually do this effectively. It is an ancient art, one that always has involved both technical and non-technical means. As more and more information and communications have gone digital, hacking has become ever more central to it. Often we call this "spying" or "espionage," terms that call to mind images of civilian agencies stealing secrets for the benefit of a government (or, in the practice of some states—though *not* the United States—for the benefit of state-controlled or state-favored private enterprises). But civilian agencies are not the only ones that engage in surreptitious information collection. When conducted by the military, we sometimes refer to this activity as intelligence, surveillance, and reconnaissance ("ISR"). ISR has connotations of informing tactical,

operational, or even strategic military planning. Whatever the label, though, the bottom line is that hacking is an increasingly-necessary aspect of stealing secrets.

- ***Covert Action:*** As our review of the CFAA underscored, the general label of "hacking" encompasses more than just unauthorized access to steal information; sometimes the access is sought in order to alter or destroy data or to cause harm to a system controlled or impacted by that data. When a government pursues that approach, a question arises regarding how to categorize the activity. Sometimes such activity will be part of an armed conflict, and we will say more about that in just a moment. For now, what matters is that not every such hack occurs in the context of armed conflict; indeed, most do not. And yet they are not instances of espionage, either. So what are they? Well, if the government involved is trying to keep its role secret, then the best answer usually will be "covert action" (there are some complicated nuances here, at least within the U.S. legal system, when the government entity involved is a military entity, but we will save that for later in the course). Covert action can encompass a wide-range of cyber operations, from information operations (propaganda, disinformation, etc.) to efforts to create damaging physical effects (sabotage).

- ***Armed Conflict***: Though journalists and others routinely refer to cyber "attacks" and "cyberwar" when talking about hostile foreign cyber activities targeting U.S. systems, the fact is that these actions rarely actually concern genuine armed conflict involving the United States. But they certainly *could*, and sometimes they really do. And so the threshold question you must ask is: Is there already a relevant state of armed conflict, or could this action on its own engender one? If not, then it is better not to talk in terms of war and combat; covert action may be the better label.

- ***Preparation of the Battlefield:*** This is military jargon for the idea that it is at times useful or even necessary for the armed forces to take certain actions in advance of potential hostilities—sometimes *far* in advance—in order to be in a better position to carry out certain operations later (that is, if and when an armed conflict actually begins). In the physical world, for example, special operators might enter enemy territory prior to a conflict in order to determine optimal routes, preposition supplies, and so forth. So too, then, with cyber operations: in order to be able to take an action involving a targeted system later, it may be wise or even necessary to establish access to that system now. Of course, in that case one most likely will be at pains to remain undetected, lest that "preparation of the battlefield" go to waste. But what if one actually wants to be detected? That leads us to the distinct concept of a "hold-at-risk" strategy.

- ***Hold-at-Risk:*** This perhaps-unfamiliar phrase is a shorthand for a simple idea. It refers to the idea that one might want to demonstrate to a rival or prospective opponent—in a very credible way—that one has the capacity to cause damage to something that they value. That is, the idea is to prove that you are holding something they value "at risk," and that the other side had best not forget this when interacting with you in other settings. Simply put, a "hold-at-risk" strategy is an effort to improve your deterrence posture in relation to an opponent, thus impacting their calculations and actions in a way that is favorable to you. In this sense, it is akin to a "show of force" in which a government puts equipment or personnel, quite visibly, in geographic position to carry out certain operations (e.g., positioning an aircraft carrier nearby). In

the cyber context, penetrating a system that contains valuable data or controls a valuable system—and allowing the other side to detect that one has done this—is a way of signaling that you truly do have the means to harm that data or system (and perhaps others as well).

- ***The Indeterminacy and Multiplicity Problems***: Here's the most important point of them all: In many instances, it is not easy for a defender to tell which of these aims might explain why someone has hacked into a particular system. To be sure, it can become clear enough once the hacker begins making use of that access in order to do certain things. But because all of the aforementioned motivations for state-sponsored hacking begin with social engineering or malware in order to gain unauthorized access to a system, a defender who has detected such an intrusion may be left with little basis for predicting what the intruder intends. Sometimes the context will help, of course, and eventually time will tell. In rare instances, moreover, external sources of information might shed useful light too. But in the meantime, the defender is left to make the best guess possible in the circumstances. Note, too, that the intruder might have in mind one purpose at one time, yet may switch to a different purpose later.

- Bearing the above in mind, perform the following exercise: **Pick a foreign power with whom the United States has particularly bad relations, imagine you are in a position of authority and trust in that government, and imagine a concrete example of an American target that you might like to have your government penetrate for each of the purposes mentioned above. Be able to explain what your country gets from each scenario, but also the offsetting risks that might give you pause.**

7. September 20 - What if the attacker is a foreign government? (II)

A. A Framework for Thinking About Threat Reduction

- Conversations about the threat foreign governments may pose to networks in the United States (including not just threats associated with formal parts of those governments like their militaries and intelligence services, but also private persons/organizations that may act on behalf of those governments) often are framed in terms of "deterrence," "escalation risk," and other familiar concepts from the international relations and security literatures. And rightly so. Before exploring those concepts in detail, however, it might help to spend a moment considering, at a high level of generality, how such concepts fit into a larger picture:
  - Let's say you are the President of the United States, and you and your advisors are formulating a strategy in response to your belief that a foreign government—let's say it is Iran—might take an action you view as a serious threat to U.S. interests. That action could involve the use of an existing capability in some unwelcome way (a use of military force, an intervention in the oil market, etc.), or it might involve an attempt to acquire some new capability that would make the foreign state a greater threat in the future (a nuclear bomb, for example). The point is: your overarching goals is to minimize the net danger.
  - To achieve that overarching goal, there are at least three subsidiary strategies you might consider (they are not mutually exclusive):

Disruption

Prevent the other state from becoming capable of taking the undesirable action. Or, if it has capability already, destroy (or at least degrade) it.

Deterrence

Defense

Minimize the harm you would suffer if the undesirable occurs. Do that by maximizing relevant

  - Note that the

disruption, deterrence, and defense strategies can relate to one another. For example: if you build strong defenses and your adversary knows this, this may cause an increase in the expected costs of the action (for they may conclude they must put more of their own resources into the effort) or a decrease in their expected benefits (for they may have to revise their odds of success). Either way, their cost-benefit assessment will be less appealing, and the degree of deterrent persuasion increased.

C. Notes on the U.S. defensive posture in cyberspace: America the vulnerable?

- ***Read this article*** by Jack Goldsmith and Stuart Russell. It details six ways in which the extensive "digitalization" of the United States results in strategic vulnerabilities that, in turn, cast a shadow over U.S. policymaking and operational decisionmaking in response to adversary actions in cyberspace. **Be able to describe each, and to explain precisely why it should matter to U.S. policymakers pondering their options in response to hostile foreign cyber activity. What larger lessons do you draw?**

D. Key terms relating to deterrence

- Some key concepts here are "Deterrence, "Cross-Domain Deterrence," "Within-Domain Deterrence," "escalation," "escalation risk," and "escalation dominance." ***Read this***. **Can you define these concepts?**
- ***Read this***. **Should the government always make public that it has taken an action in response to another state's hacking? Can deterrence work without public claims of that kind?** In answering those questions, give thought to the different possible "audiences" for such actions. Obviously one would be the foreign government to which the U.S. is responding. But who else might be watching?
- On "Attribution" in the cyberspace context, ***read this and this***. **Can you define "attribution" in this setting? Why do some claim it is especially difficult in the cyberspace context, and why would that be different than, say, nuclear weapons? What impact does such difficulty mean as to decisionmaking in particular cases?**

8. September 26 – What if the attacker is a foreign government (III)

A. Tools for imposing costs

- We have already considered the possibility of using criminal prosecution to impose costs. There are many other tools to bear in mind.
- For example: economic sanctions. This is a vast and important topic, the full scope of which is well-beyond the topic of our course. But here is what you should understand at a minimum:
    - When we talk of "sanctions" in this setting, we are referring to the ability of the U.S. government either to freeze the U.S.-based assets of a foreign person, organization, or government, or to declare some or all transactions with the sanctioned party unlawful (so, no purchases, sales, trade, donations, services, exchanges, etc.).
    - Congress at times has passed laws that directly impose sanctions, but it is much more common these days for Congress to delegate to the President the authority to impose sanctions based on certain criteria Congress sets. For example, Congress recently enacted the Countering America's Adversaries Through Sanctions Act (CAATSA, pronounced "**Cats**-uh" or "**Cots**-uh"), which among other things calls for sanctions in response to interference with U.S. elections. And definitely be aware of the International Emergency Economic

Powers Act (IEEPA, pronounced "Eye-**EEP-**uh"), which since the 1970s has served as a broad delegation of authority for the president to sanction foreign entities so long as the president has publicly declared the existence of a "national emergency" relating to a foreign affairs matter and the sanctions are related to that situation. (Note: don't be misled by the seeming-gravity of declaring a national emergency; the public over time has proven to be largely uninterested when such declarations occur, and thus it has proven relatively easy to declare them when deemed useful.)
    - By and large, presidential authority to issue sanctions under these and similar statutes ends up being delegated, through an executive order, to the Treasury Department. The body within Treasury that manages them is the Office of Foreign Assets Control ("OFAC"). Periodically, OFAC will announce new entities or individuals to be sanctioned under one or more of the currently-active sanction regimes.
    - What makes people comply with sanctions? Criminal penalties for violating them (derived from the statutes that created the sanction rules in the first place).
    - Can you sanction someone for their violation of other sanctions? Yes, that's called "secondary sanctions." This is a hot topic vis-à-vis foreign companies that want to do business with foreign entities (such as certain Iranian entities) that are themselves the subject of sanctions.
    - Unilateral sanctions (that is, those imposed only by the United States) can have an impact, but multilateral sanctions of course can have a greater impact. To get other states to follow suit, the U.S. government can try diplomatic persuasion. To actually compel other governments to follow suit? That requires a U.N. Security Council Resolution, which is no easy thing to obtain given the constellation of competing national interests the Council represents (and the fact that China, Russia, the UK, France, and the United States all have permanent authority to veto UNSC action).
- **What other tools can the U.S. government bring to bear to impose costs? Also, are their "carrots" that the U.S. government can offer instead? Generate a list.**
- To assess the deterrent value of each tool in a particular setting, you should consider at least three variables:
    - To what extent would the foreign government view the use of that tool as undesirable (to it)?
    - To what extent is it possible for the U.S. government actually to bring that tool to bear (and would the other government likely understand this)?
    - To what extent does the relevant US decisionmaker have the will to use that tool (and, more to the point, what is the other government likely to think about that)?
- Give some thought to how those variables *might* apply to each item on your list.
- We've been talking about these tools through the lens of deterrence. Above, we distinguished deterrence from disruption. **Are any of the tools on your deterrence list also useful for disruption?**

* September 27 No class (makeup session TBD) *

9. October 3 - What if the attacker is a foreign government? (IV)

Our aim at the outset of this class is to use a handful of case studies in order to understand deterrence dynamics in relation to cyberspace.

A. Russia

- ***Read*** ***this New York Times account*** from December 2016, which focuses on Russian election interference in 2016, and ***this one*** on possible responses. Next, have a look at ***this indictment*** of various Russians officers issued by a grand jury in July 2018. Questions to ponder: **How did hacking in this context relate to a larger "information operation"? What lessons does this episode suggest about vulnerability to spear-phishing? How do you assess the response of (i) the FBI in particular and (ii) the U.S. government more generally? What insights did you gather regarding the entities that conduct such activities for the Russian government? How would you characterize what Russia did here (Crime? Espionage? Covert action? Some combination, or something else?)? What would you have done differently had you been president? And, finally, is any of this actually beyond the pale, in the sense that you would not want to see the United States doing the same thing (and do you see how that is a different question from asking whether the United States should do what it can to stop such actions from succeeding against it)?**
- ***Read*** ***this Washington Post story*** regarding another Russia incident, ***the resulting indictment***, and the ***latest developments*** in the case. **How do you assess the effectiveness of the U.S. government response in this instance? Can the same model reliably be applied elsewhere?**

B. China

- ***Read*** ***this Christian Science Monitor piece*** examining Chinese-government sponsored hacking against U.S. targets (public and private) in recent years. **How does Chinese-government sponsored hacking differ from the Russian activities descried above, and what follows from this as a matter of policy? Should it be off-limits to hack businesses in hopes of providing competitive advantages for your own nation's companies (and does it really matter if the companies in question, on either end, are formally owned in part or in whole by the state)? Should the United States have done more to respond to these hacks?**
- The Obama administration surprised many observers when it brought criminal charges against a group of PLA hackers (*United States v. Dong* (W.D. Pa.). ***Read*** ***the indictment***, as well as ***this story*** and ***this story*** about the case. Analysis of the impact of this effort has been conflicted. ***Compare*** ***this account*** and ***this account***. **What lessons if any do you draw from this? Is prosecution an effective approach? Scalable? Does news of *this recent arrest* –possibly linked to the famous OPM hack—change your view?**
- Prosecution is not the only tool available, of course. ***Read*** ***this Executive Order*** from President Obama, which in April 2015 established a system for sanctioning the beneficiaries of cyberespionage used for commercial advantage. **Read more *here*** and ***here***, too. **Pros and cons of this approach?**
- Eventually, the U.S. and Chinese government struck a deal, of sorts. What was it, and has it helped? ***Read*** ***this recent account***. **What lessons do you draw?**

B. Encouraging Potential Victims to Better Protect Their Systems

Minimizing unauthorized (and excessive) access is not just a function of imposing painful consequences on intruders. It is also a function of making it harder for them to succeed when they do make the attempt—*i.e.*, improving defense. Indeed, recall how we distinguished disruption, deterrence, and defense in the readings above. Improving defense will, at the margins, prevent some intrusions in the sense that some attacks that might otherwise have succeeded will now fail. Moreover, even for attackers who are able and willing to overcome the improved defense, the improvement increases the attacker's costs, thereby making the effort marginally less attractive (by reducing prospective return on investment) and perhaps even causing the attacker to reduce the scope of their activities due to resulting resource constraints (sometimes this is called "deterrence by denial"). Incentivizing potential victims (whether they are private or public entities or individuals) to improve their defenses on a systemic basis thus can serve an important goal of cybersecurity policy.

Of course, most potential victims already have at least *some* incentive to develop and improve defenses even absent any form of government intervention. Some have trade secrets to protect. Some desire to keep things private. Some need to keep customers happy. And so forth. As a result, we can safely assume there will be *some* defensive activity even if *no* external forces intervened to encourage such steps. It's rather like the situation of a building owner. Most owners would take at least *some* steps to make the building safe even if there were no building codes, insurers, or plaintiff's lawyers with which to contend.

But is this "natural" level of effort good enough? In the building context, society has answered that question with a resounding no; governments, insurers, and litigators intervene in all sorts of ways to spur further safety measures in that setting. And the same is true with respect to various other contexts, such as pollution and public health. In these and other settings, we see extensive market interventions in the name of safety (whether all such interventions are genuinely so motivated is an entirely different question beyond the scope of our course).

Increasingly, we are doing the same with respect to cybersecurity.

As we shall see, the levers for intervention are pretty much the same in all these contexts (though it is much more interesting to study them in the cybersecurity context, since they are much newer and more-contested here). We will focus on four of them.

The first two—regulation and liability—are familiar to most of us. We will start by examining the *regulatory* approach: that is, top-down imposition of rules (via statute or through regulations promulgated by an agency) that just directly require that certain entities employ particular practices or procedures, upon pain of facing some form of enforcement action (usually in the form of a civil suit brought by a regulatory agency). Our aim is to understand whether and how the United States has embraced this approach to driving better defense, and what forces explain the status quo. Next, we will turn to consider the *liability* approach quite apart from the actions of regulatory agencies. That is, we will consider the extent to which organizations or individuals may be exposed to private lawsuits for money damages (usually brought by the downstream victims of data breaches, such as customers and credit-card issuers) if some entity arguably had inadequate defensive measures.

The next two mechanisms are less-familiar, yet easy enough to grasp. First, insurance. The availability of insurance coverage in the first instance (not to mention the details regarding when a claim actually will be honored) can be a powerful incentive for behavior in this context as much as any other. Second, we will consider what one might call "pruning": identifying ways in which the current legal architecture unintentionally disincentivizes some

desirable defensive measure, and then altering the law to remove that disincentive and hopefully pave the way for voluntary improvements.

Next, we will look at a pair of considerations involving the federal government in particular. Under that heading, we first will consider the government's role in mandating improved defenses for…itself. The federal government consists of a vast array of distinct institutions, and each of them has its own array of information systems to protect. However hard it may be for the government to compel *other* entities to do better at defending *their* systems, it should be easier for it to compel its own constituent parts to do so. We will examine how that responsibility is distributed within the government, and we will consider how effectively it has been executed in recent years. Separately, we also will consider how the federal government has an additional capacity to incentivize improved security by others, thanks to the considerable leverage that some parts of the government wield through their purchasing and contracting authorities.

10. October 4 - The Role of Regulators: Rulemaking & Enforcement
11. October 10 - Same

A. About Federal Administrative Agencies

- The federal government contains a large number of administrative agencies. Each has some particular field of subject-matter responsibility (the scope of which is defined by statute in most cases). Each typically performs many functions, but we are especially concerned with two core capacities.
- First, rulemaking. An agency might have authority to promulgate legally-binding regulations (that is, to engage in "rulemaking") in furtherance of some goal specified by Congress. For example, Congress has given the Environmental Protection Agency authority to promulgate regulations to further the goals of the Clean Air Act in certain ways. There are a host of complex procedural rules associated with agency rulemaking, but for now it is enough to know that this has been a common mode of creating law since the 20th century.
- Second, enforcement. Congress sometimes authorizes an agency to initiate and pursue "enforcement" proceedings. The idea is that the agency may be tasked with investigating possible rule violations (whether a rule stated directly in a statute enacted by Congress, or a rule promulgated by an agency pursuant to authority delegated by Congress) and then initiating civil proceedings to enforce alleged violations. In some cases, the enforcement action might take the form of an ordinary civil suit, with the agency suing the alleged violator in federal court. But sometimes Congress empowers the agency also or instead to adjudicate the enforcement process internally (at least as an initial matter), with a litigation process involving an administrative law judge within the agency itself. Either way, the general idea is to secure a determination that someone violated a rule, producing a costly fine/damages, an order obliging (enjoining) the violator to take or cease some particular action(s), or both.
- Like other forms of litigation, agency enforcement proceedings routinely result in settlements in which the alleged violator agrees to take or cease certain actions, with the possibility of more severe consequences later on if the party breaches that obligation.
- Note that other parties in an industry may take note of the initiation and resolution of enforcement actions; they cast a shadow—sometimes a very long shadow—that may impact how other players decide to act. **Bearing that in mind, can you make an argument that "enforcement" authority is itself a second form of rule-making authority?**

B. There Is No Cybersecurity Protection Agency (Yet)

- I mentioned the EPA above. It was created during the Nixon Administration at a time of mounting concern about the harmful effects of pollution. Over time, Congress has granted various rulemaking and enforcement authorities to the EPA in furtherance of this general mission. One might argue that mounting concern about inadequate cybersecurity warrants creation of a similar dedicated agency. It is important to grasp, however, that Congress so far has not taken that step.
- But that does not mean that there are no agencies engaged in promotion of cybersecurity. It just means there's no new agency created for and dedicated exclusively to this purpose.
- Your goal in light of all that: understand how certain pre-existing agencies have managed to participate in cybersecurity promotion. We'll start with the one you hear about the most in this space: the FTC.

C. The Federal Trade Commission ("FTC") and the FTC Act

- For a very brief introduction to the FTC, read this. Based only on this overview, would you expect the FTC to have a role in setting or enforcing standards for cybersecurity? Why or why not?
- One of the statutes the FTC is empowered to enforce is the Federal Trade Commission Act ("FTC Act"). The FTC has *not* engaged in any rulemaking relating to cybersecurity under this statute. Instead, it has focused on enforcement actions, based on the claim that some situations involving poor cybersecurity violated a rule set forth in the FTC Act itself. In fact, it has initiated more than 60 enforcement actions along these lines, and has touted the resulting body of cases as functioning, collectively, as a form of guidance to the private sector. In a moment I'll ask you to consider whether this level of enforcement, without tailored rulemaking, is desirable. But first you need to know just what they've been enforcing and how they've been doing it.
- Goal #1: Understand what exactly the FTC Act prohibits. The answer is found in **15 U.S.C. 45(a)(1)**. Read just that part—(a)(1)—carefully. There's an opening clause about unfair competition, and a second clause that refers alternatively both to "unfair" practices and "deceptive" practices that impact interstate commerce. **Can you explain how unfairness is different from deception? Does either concept seem relevant to a situation in which some entity has poor cybersecurity? In terms of clarity (and thus understanding on the part of those who must comply), how does this compare to the various subparts of the CFAA?**
- Goal #2: Understand how **15 U.S.C. 45(n)** limits one (but not both) of those two prohibitions. **Which one is impacted, and is the impact likely relevant for a cybersecurity situation?**
- Goal #3: Understand whether there are significant limits with respect to who has to care about the FTC Act. **Read 15 U.S.C. 45(a)(2). Does it encompass everyone?**
- Goal #4: Understand how the FTC goes about enforcing the FTC Act. It has two available options. **Read 45(b) and 45(m)**. **Can you explain the difference between the two procedures in terms of who decides whether the FTC's allegation is correct? In terms of what remedies appear to be available if the FTC wins?**
- Case study: Uber
  - **Read this complaint** filed by the FTC. **Which enforcement path did the FTC use in this case? In what way(s) did Uber allegedly violate Section 45(a)? Assuming all the allegations to be true, would you agree with the FTC that this violates the statute?**
  - Eventually Uber settled with the FTC, but then in April 2018 the FTC announced it had reopened the case due to Uber's failure to disclose that, during the pendency of the case at the earlier stage, Uber had experienced another data breach. This led to a revised settlement agreement. **Scan the document** to get a sense of the

commitments FTC extracted from Uber. **What are they, and was this a good outcome?**
    - The FTC was not the only problem Uber faced in connection with these events. A number of state Attorneys General decided to team up and sue Uber together, based on various state data-breach liability laws we will examine in the next class. For now, it is enough to note that Uber faced this massive and well-resourced lawsuit at the same time that it faced the FTC's renewed enforcement action. **Consider how the pendency of parallel litigation might matter.** Oh, by the way, Uber and the states have just announced (9/26/18) that they are settling for $148 million
- Case Study #2: Wyndham Hotels
    - Here's an example of the FTC suing in federal court. **Read** this note summarizing the litigation involving Wyndham Hotels. **What was Wyndham's argument about the propriety of suing them under the "unfairness" prong of Section 45(a)(1)? How did the court rule on that point, and do you agree? What was Wyndham's second argument, concerning "fair notice"? How did the court rule on that one, and do you agree?**
    - Note: Wyndham and the FTC settled later, with Wyndham agreeing to take on a variety of security-focused practices (as well as annual audits) for the next 20 years.
- Case Study #3: LabMD
    - This was a remarkable case in many respects. I won't summarize it here, but rather will ask you to **read this short overview** from Prof. Dan Solove. **Can you summarize how the outcome in *LabMD* compares to *Wyndham*?**

D. The FTC and the Gramm-Leach-Bliley Act

- As it happens, the FTC also has authority to enforce other statutes, and in some cases to promulgate regulations relating to them. One such statute is the Gramm-Leach-Bliley Act (the "GLB Act"), which among other things concerns the protection of customer data by financial institutions.
- The FTC has promulgated a set of regulations on that issue, known collectively as the "Safeguards Rule" (found in 16 Code of Federal Regulations Part 314). **Skim the text of Part 314 and then read this FTC-written overview. Who does this govern, and (at a general level) what does it require them to do?**
- For a recent illustration of the Safeguards Rule in action, **read** pp.3-5 of this action the FTC pursued against TaxSlayer. I won't have questions for you about this one; it's just an illustration.

E. A Quick Look at Other Federal Regulators

- There are other federal regulators involved in cybersecurity, besides the FTC. We will not go into anything like the same level of detail with them, but you should have at least a glancing familiarity with the roles some of them play.
- For each example below, **identify the substantive standard that the agency appears to be enforcing**:
    - **Read** here for an example involving the Securities & Exchange Commission ("SEC").
    - **Skim** this (just glance through the first dozen pages) for an example involving the Federal Communications Commission ("FCC").
    - Note that medical devices obviously raise especially-acute cybersecurity concerns, particularly when the device in question can be accessed remotely and is capable of causing significant harm. I'm not assigning you anything relating to the Food and Drug Administration (the "FDA"), but if you are interested in going deeper on this topic: do some searching to see if you can determine whether the FDA has gotten involved with cybersecurity regulations or enforcement.

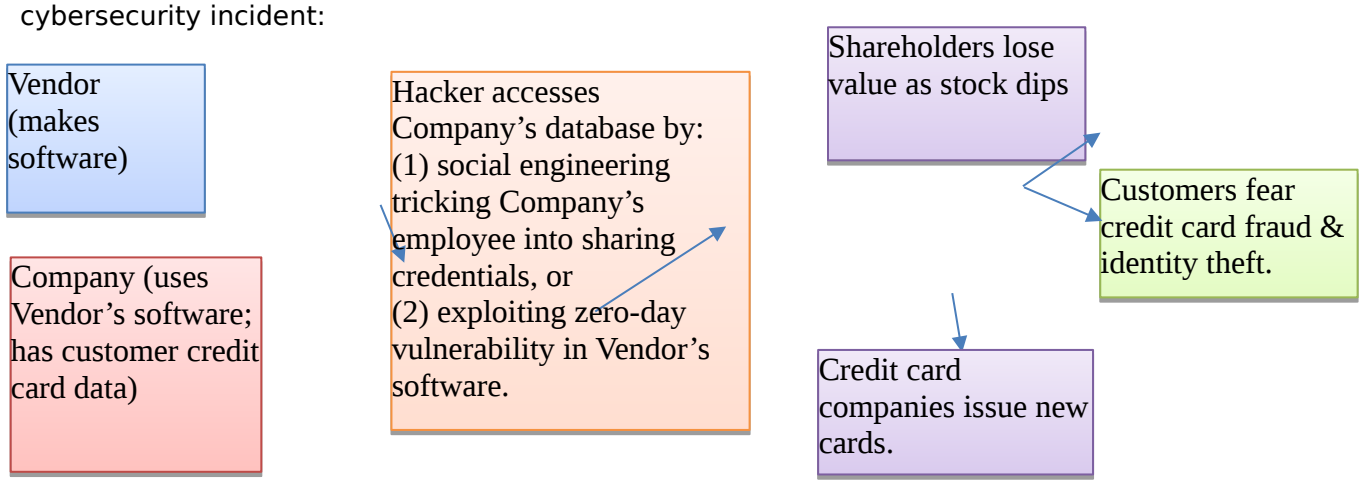
F. Don't Forget the State Regulators and Foreign Regulators

- Why should all the fun be left to federal regulators? Of course, it isn't. I want you to be generally aware of various ways in which other regulators become involved, though I'm not going to ask questions about this in class or hold you accountable on the exam for it. This is just for your general awareness. This example recently took effect in New York in relation to the financial services industry. And here's a short piece explaining how various European regulators responded to the same Uber breach we noted above.

12. October 11 The Role of Private Lawsuits and Insurance

A. The Big Picture: Who Are the Injured Parties Who Might Become Plaintiffs?

- Consider the following depiction of the chain of actors involved in a common type of cybersecurity incident:



- **Who would you characterize as a victim?**
- One might expect that, if anyone is to be sued for damages, it would be the hacker. That rarely occurs, however. **Why might that be?**
- Usually the vendor is not sued either. That's to be expected if the hacker breached the company's security via social engineering; that's a failure on the part of the employee(s) and perhaps the company, but not the vendor. But what if the breach was the result of a vulnerable in the vendor's software? **Read this article and make a list of the obstacles to suing software providers.** Consider the policies that might be served by each obstacle. **Would you change any of them?**
- This leaves the option of suing the company that actually suffered the breach. Our goal now is to understand the major form so liability that companies in this situation might face.

B. Tort Liability (For Lack of Due Care)

- In our legal system, we use the word "tort" to refer to situations in which the law authorizes suits for damages based on harmful actions/omissions. Some torts are "common law" causes of action, meaning that the courts have recognized a right to sue in a particular situation even without a statute calling for recognition of that tort. This is the traditional and most familiar kind of tort. Examples include negligence and battery. But legislatures can create torts by statute, too, if they wish.
- There are many kinds of torts. One batch, called "intentional torts," involves purposefully-harmful conduct. That's not our concern here, for we are assuming that companies do not intend to be breached. So that leaves us with unintentional harms. In that situation, the tort system can take either of two approaches. First, it can make

someone strictly-liable for all harms they cause. Second, it can make them liable only for harms that result from lack of adequate care—what we commonly call "negligence." The strict-liability approach is relatively rare, and usually confined to ultra-hazardous activities. For companies that may have inadequate information security, the important question is negligence.

- As all law students learn during their first year, negligence makes a defendant liable in damages where four conditions are met: (1) the defendant owed a duty of care, (2) the defendant breached that duty, (3) the plaintiff suffered a legally-recognizable harm, and (4) the breach was the proximate (reasonably-foreseeable) cause of that harm. **Pause now to consider how, in the scenario above, the company's customers *might* have a negligence claim against (a) the company or (b) the vendor.**
- Case study #1: A Negligent Law Firm?
  - **Here is an illustration** of a suit against a company—a law firm, actually—for negligence relating to inadequate information security. Assume the allegations are true: **Do you think the elements of negligence are satisfied?** Note how the plaintiff used the defendant's own words against it when describing its view of what should count as due care in this context.
  - Even if the plaintiff seems unlikely to win on the merits if the suit goes to trial, the defendant still might conclude that the rational path forward is to settle the case. **Why, and what does that suggest about the incentives created by the possibility of being sued?**
- Case study #2: Equifax
  - Not long ago, Equifax (one of the major credit-reporting agencies) suffered a massive data breach. Credit-reporting agencies are a particularly-appealing target for this sort of thing, in light of the vast volume and sensitive nature of the information they collect. As you might imagine, news of the breach made headlines, and many lawsuits followed. **Here is the complaint in one of those case**.
  - The plaintiffs in this case seek "class action" status—that is, they seek approval from the court to assert not just their own claims but those of all other similarly-situated persons. **Consider the pros and cons of class-action status from the point of view of the defendant, the plaintiff, and the plaintiff's attorneys** (bearing in mind that the plaintiff's attorney most likely are being compensated on a "contingent fee" basis—meaning that they will receive a percentage of the eventual recovery, if any).
  - It can be hard to prove what the duty of care is, let alone that a breach of it occurred. But in the data breach context, the real challenge often is showing damages proximately caused by the breach. **Read this** for a critical perspective on that problem. **Do you agree with EFF?**
- *Breach of a Statutory Duty of Care*[1]
  - *The question of whether and to what extent tort liability should exist for failing to secure data sufficiently does not have to be left up to the common-law process in which courts consider whether to recognize a duty of care in this space. If a state legislature wants to confirm that such liability exists, it can do so by statute. And California recently did exactly that.*
  - *Section 11 of the California Consumer Privacy Act of 2018 (codified at Cal. Civil Code Section 1798.150) provides that certain companies doing business in California are subject to civil suit for injunctive relief or damages (in the amount of the plaintiff's actual damages or else "statutory damages" (that is, a pre-set penalty determined by the statute) in the range of $100-$750 per consumer per incident, whichever turns out to be higher) if "nonencrypted or nonredacted personal information…is*

1 This is material we discussed in class, though it was not included in the earlier version of the syllabus. I've added it to the syllabus now both for the sake of convenience for those who were in class that day and for the benefit of those who for whatever reason missed that class.

subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation ***of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information….****"*

- ***How does this statutory standard compare to common-law negligence?***
- ***In light of how the statute describes the category of information subject to the statute's protection, what advice would you give to a company that has personal information to protect?***

C. Contract Liability (For Failing to Live Up to Security-Related Promises)

- In some settings, the company that suffered a breach will have made security-related representations in a contract of some kind. A professional-services firm, for example, might include such representations in the "engagement letter" that serves as the contract between the firm and its clients (sophisticated clients increasingly will insist upon this). In other settings, there may be terms-of-service that govern a customer's or user's relationship to a company (particularly but not only where customers or users interact with the company via an app). These too may contain security-related representations. These and other examples create the possibility of a breach-of-contract lawsuit in the event of a data breach where the breach arguably shows that the company failed to live up to its promises.
- Of course, companies make some representations in settings that do not count as part of a contract with a customer or user. For example, a company may make statements in advertisements or on their websites, including statements about care they take to protect customer and user data. **Consider how this illustrates the difference between a breach of contract claim and an FTC enforcement action based on deceptive advertising.**
- Case study #3: Anthem
  - In February 2015, the health insurance company Anthem announced that its security had been breached and that a massive amount of personally-identifiable information about patients had been exposed. This led to massive litigation, based on a variety of claims including breach-of-contract claims. Anthem tried to have these claims dismissed, but was only partially successful. On one hand, it *did* succeed in having the breach-of-contract claims dismissed, on the ground that the promises it made on its website's "privacy statement" and in certain mailings to customers, regarding customer privacy, were not actually part of a contract with customers. On the other hand, the court refused to dismiss a separate cause of action, under California state law, for deceptive advertising.
  - Having failed to get the whole case dismissed, Anthem eventually settled. **Read about it here. What did the plaintiffs receive? What did the plaintiff's *attorneys* receive? How do you feel about this result?** Also **read this more-recent notice** about the settlement.
  - By this point, you surely are asking yourself: Didn't the regulators from last week also get in on the Anthem action? Of course they did!
    - Because Anthem was in the insurance business, a California state insurance regulatory agency conducted an investigation. The summary of its report is quite interesting. **Read the summary here. Is this inconsistent with the civil litigation result? If so, is that a policy problem and what might be done about it?**
    - As for the FTC: It did not get involved. But because Anthem was involved in health matters, another federal agency did: the Department of Health and Human Services ("HHS"). For a quick glance at HHS's role in this space, **read this.**

D. Liability for Inadequate Disclosure of a Data Breach

- The possibility of being sued for inadequate care, failing to live up to a promise, or deceptive advertising all loom large when a company learns that it has been breached and that customer or user data has been exposed. And that in turn creates an incentive for the company leadership to proceed very carefully—and thus very slowly—in letting anyone know that the breach has occurred. But there is a powerful consideration pushing in the exact opposite direction: all states have laws compelling companies to disclose such breaches, and to do so rapidly. **Can you summarize the competing public-policy interests implicated by such laws, and how you assess the balance between them?**
- Needless to say, we are not going to look at all the different state breach-disclosure laws. Instead, we'll look at Texas law as an example. **Read Texas Business and Commerce Code Section 521.053(b).**
  - **How certain must the entity be that a breach occurred?**
  - **Precisely how quickly must the disclosure be made as a default matter?**
  - **How does section 521.053(d) potentially change that timeline?**
  - The Texas Attorney General is responsible for filing civil suits to enforce Section 521.053, but note that a Section 521.053 violation may also constitute a deceptive act for purposes of a private civil suit under the Texas Deceptive Trade Practices Act.
- As you might imagine, the patchwork quilt of disclosure laws around the various states (as well as some cities) has led some to argue for Congress to impose a uniform national approach. **What are the pros and cons?**
- Don't forget: some companies will be subject to foreign jurisdictions as well, and these may be more demanding than American disclosure requirements. The European Union's much-discussed "General Data Protection Regulation" ("GDPR") is a particularly-significant example you should be aware of (though we are not studying its particular requirements in this class).

E. Shareholder Derivative Actions

- Recall that in our generic scenario above, we noted the possibility that Company B has shareholders who might sue it, assuming share prices dropped once the breach became public. Such "shareholder derivative actions" arise frequently with publicly-traded companies, when those companies experience any sort of significant reversal that might be attributed to bad decision-making by the company's officers or board of directors. **Read this article for a fine overview of how such suits have fared in some of the most well-known data-breach cases.**

F. Insurance

- In any context in which entities and individuals can anticipate suffering a loss—whether the loss be from damage to possessions or person, or from at least some forms of legal liability—there is a strong incentive to protect against the anticipated loss by purchasing an insurance policy. Because insurers usually (though definitely not always) are at liberty to determine which sorts of risks they will insure against, and subject to which conditions, the insurance industry in general is in a powerful position to nudge or even compel certain behaviors (just think of the incentives for safe driving that car insurance does or might generate). And thus insurance has an important role to play in relation to the general challenge of encouraging potential victim's to engage in better defense. For a handy and accessible (and brief) introduction to the emerging cybersecurity insurance market, **read this testimony from a leading insurance executive** before a Congressional hearing in July 2017.

13. October 17 Pruning Disincentives and Leveraging Purchasing Power
14. October 18 Same

A. What Do We Mean by "Pruning" and Where Does It Matter for Cybersecurity?

- In some situations, an entity might be willing (perhaps even eager) to pursue some particular security measure, but is deterred from doing so by the potential applicability of a legal constraint (criminal, civil liability, regulatory pressure, etc.). In such circumstances, "pruning" the law to remove that perceived constraint might be an effective means of incentivizing better security; think of it as addition-by-subtraction. The trick, of course, is that the law in question likely serves a competing interest, and hence potential security gains might come at a significant cost to other worthy values.
- One area in which pruning might help, for cybersecurity purposes, involves information-sharing.

B. What Sort of Information Might Be Shared?

- We are concerned here with what I will call "threat intelligence," but be sure to appreciate that this is a term of convenience rather than a term of art with well-settled meaning and scope. That said, what does it encompass? At a minimum, it includes "Indicators of Compromise" (aka "IOCs"). IOC is a shorthand for the idea that there are technical signatures and other tells that reveal unauthorized activity. This could be the "signature" for known exploits, or the URL of a known botnet command-and-control server, etc. Sometimes you'll see the phrase "threat indicator" used for this type of intelligence. But "threat intelligence" for at least some people has a broader scope, and might encompass other useful information, both of a technical variety (for example, details about a newly-discovered vulnerability or patch) and otherwise (for example, information about the capabilities, motives, intentions, or characteristic tactics, techniques, and procedures of potentially-hostile entities or individuals). **Be able to define and apply these categories.**
- Rapid dissemination of technical threat intelligence (IOCs, new vulns, and patches) is critical. It's just like ensuring widespread and rapid uptake of a vaccine. **Understand how cybersecurity is, in this sense, akin to a public health issue.**
- Be alert to the possibility of miscommunication when someone makes a general reference to information sharing, and specifically for the possibility of confusion regarding what subtypes of information is in issue.

C. Why is Information-Sharing Difficult, in Theory?

- Information sharing can be government-to-government, government-to-private, private-to-government, and private-to-private. Each presents its own challenges, and overall there is a question here about why we might not get sufficient sharing without government intervention. **Why would one government entity be reluctant to share information with another, within our own government or across governments? Why would the government be reluctant to share with the private sector, and vice-versa? Why might one private entity resist sharing with another? And do your answers depend on which subtype of "threat intelligence" is at issue?**

D. Pruning and Facilitating: The Cybersecurity Information Sharing Act of 2015

- In 2015, Congress passed and President Obama signed a bill that included the "Cybersecurity Information Sharing Act of 2015" (generally known as "CISA"). The full text of that **bill is here, but don't read the whole thing.** Instead, **look at specific provisions within it** as follows:
  - Section 103: **What exactly does this section oblige DNI, DHS, DOD, and DOJ to do in relation to information-sharing?**

- Section 104(c): **What legal limitation(s) does 104(c)(1) overcome? What is the point of the caveat in 104(c)(2)? And why include the language in 104(c)(3)?**
- Section 104(d)(1) and (2): **What burden does (d)(1) create, and can you relate this to any of the existing duties/burdens we studied the prior two classes? What obligation does (d)(2) impose?**
- Section 104(e): **Why was this provision necessary?**
- Section 105: This one is long. **Review it carefully to decide what its most important functions are. Then read this document to understand how the agencies have responded to section 105. Does this leave you with any concerns?**
- Section 106: **What legal obstacles does this section prune? Does it go too far, not enough, or just far enough?**
- Section 108(i) and (k): **What are the effects of these provisions?**
- **Does this likely address all potentially-significant legal hurdles to sharing?**

E. A Closer Look at Whether and How Information-Sharing Occurs

- **Read this paper** from Elaine Sedenberg and James Dempsey.
- **What is the purpose of an ISAC? And how is an ISAO different?** Go online and see if you can locate examples of each; **what do they appear to do?**
- **Can you identify other entities or arrangements that facilitate information sharing?**
- **What are the pros and cons of this diverse "ecoysystem"?**
- **Do the authors find CISA's pruning useful? Why or why not, and are you convinced?**
- **What other lessons do you glean from this paper?**

F. Better Security By Leveraging Government Contracting/Purchasing Power

- Before we move on, let's pause to note another significant tool that the government sometimes can wield to compel potential breach victims to improve their cybersecurity: putting demands for such improvements into the terms of significant government contracts.
- **Can you see how this is analogous to the leverage wielded by insurers?**
- Here's an example involving an attempt by the government to leverage contracting power to keep certain private entities from using the antivirus products and other services of Kaspersky Lab (a Russia-based AV vendor that once had a substantial share of the US market, and still has a large global presence). **Can you identify limits to the utility of this approach, based on this example? What are the pros and cons?**

15. October 24 Getting the Government to Protect Itself Better
16. October 25 same

In recent classes we have surveyed the set of tools that can be used to incentivize private sector entities to adopt stronger security measures. But what about the *government's* own security practices? How do we get it to defend better?

The "government," of course, is not an "it." The word "government" encompasses a vast array of distinct enterprises, any one of which may operate any number of separate networks, databases, etc. Even if we limit our focus to the U.S. government (leaving aside states, counties, cities, tribal governments, territorial governments, and so forth), the number of relevant actors is bewildering. Like the private sector, these entities have internal incentives to maintain the security and functionality of their systems (for example,

the SEC does not want people to access private information and thus enable market manipulation, just as NSA does not want Russia to be able to learn its techniques and capabilities). But also like the private sector, we have ample reason to believe that, if left to their own devices, many if not most government entities would not—or perhaps could not—invest as much in security as they should. And so, again like the private sector, we need tools to compel these entities to try harder.

Our goal in this class is to understand the basic elements of those tools: what they are, who is in charge of them, and how they came about as a historical matter. But before we dive into all of this, let's make the subject concrete with a quick glance at a particularly-painful infosec failure for the federal government: the 2015 Office of Personnel Management ("OPM") hack.

A. The 2015 OPM hack as a case study

- The most well-known data breach involving a U.S. government system involves the hugely-successful operation in which Chinese hackers breached security at the Office of Personnel Management and thereby acquired a vast trove of security-clearance background check files. We could spend days and days learning the details of what occurred here, especially if I had you read the 241-page report that resulted from the Congressional investigation into this episode. But our aim here is limited, and so instead just **read this article** in order to answer these questions:
  - When we ask "how the attack" happened, one can answer either by explaining which vulnerabilities were exploited or by referencing larger factors that might explain why both the vulnerability and the exploitation went undetected for so long. Let's consider both those questions.
    - As a technical matter: **how did intruders gain access to OPM's system, and—perhaps more importantly—what factors explain their ability to then move about within and extract data from the system?**
    - In terms of the larger factors that made this possible: **Can you imagine factors (such as expertise, management, bureaucracy, budget, legal requirements, policy requirements, culture, personality, and so forth) that might explain why the technical failings were possible?**
    - **If you were called upon to "fix" these large factors in the aftermath of this episode—and thereby hopefully reduce the chances for a repeat—what might each fix entail? And what considerations might make a particular fix difficult to implement?**
  - As long as we have this case study cued up, let's use it for a quick review:
    - **Can you categorize the OPM hack using the typology of government actions we reviewed earlier in the course?**
    - **In light of that categorization and drawing on our prior discussions of US-China relations, how should the U.S. government have responded? *Think of three specific potential actions, and list pros and cons for each*.**

B. Incentivizing improved government security: Does litigation risk help?

- As we saw previously, one way to encourage defensive improvements is to increase the extent to which entities perceive that they are exposed to litigation risk for potentially-inadequate security. It works with private sector entities. Can it work with the government itself too? In theory, sure. But as things currently stand, government agencies do not face significant exposure as a practical matter.
- First, note that government agencies do not have to worry about getting sued by…other government agencies. The FTC, state attorney general offices, and the like may loom large for private businesses, but they do not haul their fellow government agencies into court (let alone into their internal enforcement systems. And, similarly, government agencies typically does not have to concern themselves with what insurers think.

- What does that leave, from a litigation-risk perspective? Government entities *do* face the possibility of suits brought by private plaintiffs. But such suits have a bad track record. Our goal now is to understand why.
- The first problem is "sovereign immunity." Unlike a private entity, federal and state government entities cannot be hauled into its own courts involuntarily; as sovereigns, they can only be sued if they have consented.
- Does that ever happen? Yes, in fact it is common. Both federal and state laws are full of examples of statutes expressly waiving immunity as to certain types of claims. The question for us is: Do any of them apply in a setting where the government entity had poor cybersecurity? There are some that *might*, but in practice they've not yet proven to have much bite in the cybersecurity setting.
- The most well-known statute of this kind at the federal level is the Federal Tort Claims Act. It waives immunity where a person suffers personal injury, property damage, or death as a result of wrongful or negligent conduct by a government official. Most states (including Texas) have something similar on the books. It is difficult to use these laws to sue successfully for damages relating to a data breach, however, in light of the injury requirement.
- Other possibilities plaintiffs have tried include the Privacy Act and the Little Tucker Act (seriously, that's its name). Again, though, the track record is dismal. Both those statutes (along with several others) are central to a lawsuit filed in the wake of the massive Office of Personnel Management ("OPM") hack (involving the theft of security-clearance background check data). The case, known as *In re U.S. Office of Personnel Management Data Security Breach Litigation*, is going poorly for the plaintiffs. In September 2017, in a ruling that currently is under appeal, the district judge granted the government's motion to dismiss all claims, including claims under those two statutes, explaining:
  - The Privacy Act (5 USC 552a): The Privacy Act is meant to regulate how government agencies manage their records, with an eye towards protecting the privacy of individuals in a way that is compatible with the need for agencies to make use of such information for proper purposes. Among other things, the Privacy Act authorizes private suits for situations in which an agency willfully or intentionally fails to adhere to Privacy Act rules and, as a result, the plaintiff suffers actual economic/pecuniary damage. The district court concluded that most of the plaintiffs in this case had alleged no such damages, and as for the two who did allege such harm (in the form of alleged identity theft) the allegations failed to link the harm to OPM's data breach.
  - The Little Tucker Act (28 USC 1346): This statute is analogous to the Federal Tort Claims Act, but instead of permitting tort suits against the government it permits breach-of-contract actions. The plaintiffs suggested that the government implicitly (or perhaps even expressly) contracted with them to protect the data provided during the background-check process. The district court concluded, however, that there was no relevant contract between the government and the individuals whose data was exposed in the OPM hack.
  - **Should Congress adjust one or more of these laws in order to approve the prospects for private litigants challenging government agency security practices?**
  - **Even if it does so, is it clear that the increased exposure would impact agency decisionmaking in a manner similar to the way that litigation risk may impact the decisionmaking of private entities?**

<u>C. Directly Requiring Better Security: The Role of Government Self-Regulation</u>

- It may be that litigation risk is never going to play a major role in encouraging government agencies to try harder, but there are other tools in the toolkit. The one that looms largest with respect to the government's own cybersecurity is self-regulation.

- Note that we previously observed that the private sector likely would not pursue security aggressively enough if every private entity was left to its own devices. **Why should we expect self-regulation to be more impactful when it comes to public-sector entities?** Hint: Remember that the government is a "they" and not an "it," meaning that there are many different entities in complex relation with one another in "the government"—and "self-regulation" in this context accordingly might better be described as "cross-governmental regulation."
- Our goal now is to understand the most significant current sources of government self-regulation, seen in historical perspective. More specifically, let's look at the government-wide policies that have been imposed both by statute and by executive order.
- Let's start (somewhat arbitrarily) in 1996, during the Clinton administration. A statute passed that year tasked the Secretary of Commerce with establishing information-security standards that the rest of the government would henceforth have to follow (well, not everyone; defense and intelligence agencies were left to follow their own rules in this respect). The statute specified that the Secretary should base his or her directives on the standards and guidelines developed by the Commerce Department's National Institute of Standards and Technology (better known as "NIST"), which is a deeply-respected technical organization.
- Fast-forward six years, to the early years of the George W. Bush administration. In 2002, Congress passed the Federal Information Systems Management Act of 2002 ("FISMA," pronounced "**fiz**-muh"). FISMA updated the 1996 law, shifting the standard-setting role from Commerce to the White House's Office of Management and Budget (OMB) while also clarifying that OMB would not just set standards but also would review agency compliance with those standards on at least an annual basis.
- Significantly, FISMA 2002 also directed the creation of an "information security incident center" that would both provide expert advice (including in the face of an unfolding emergency) and function as a threat intelligence hub (collecting and analyzing information. This eventually became US-CERT ("Computer Emergency Response Team"), which today is housed within DHS. This was not a matter of improved-defense via self-regulation, of course, but rather one of improved-defense via capacity-building.
- After another six years, in 2008, President Bush issued National Security Presidential Directive 54/Homeland Security Presidential Directive 23. NSPD 54/HSPD 23 called for DHS (then still a relatively-new agency, as it was created by legislation in 2004) to play the lead role in protecting federal networks. Among other things, it directed DHS to act through US-CERT to monitor and protect all "external access points" associated with federal government systems, and to provide intrusion detection, incident analysis, and other capabilities. Again, this was not a matter of self-regulation, but rather one of capacity-building.
    - DHS responded to this assignment by, among other things, developing and deploying an intrusion-detection system labeled "Einstein." Here is an account of Einstein versions 2 and 3 from a few years ago(full source here, but just read the excerpt below):
        - …DHS is deploying, as part of its EINSTEIN 2 activities, signature-based sensors capable of inspecting Internet traffic entering Federal systems for unauthorized accesses and malicious content. The EINSTEIN 2 capability enables analysis of network flow information to identify potential malicious activity while conducting automatic full packet inspection of traffic entering or exiting U.S. Government networks for malicious activity using signature-based intrusion detection technology. … EINSTEIN 2 is capable of alerting US-CERT in real time to the presence of malicious or potentially harmful activity in federal network traffic and provides correlation and visualization of the derived data. [Meanwhile, DHS is developing a new system], called EINSTEIN 3, [that] will draw on commercial technology and specialized government technology to conduct real-time full packet inspection and threat-based decision-making on network traffic entering or leaving these Executive Branch networks. … The EINSTEIN 3 system will also support enhanced information sharing by US-CERT with Federal Departments and Agencies by giving DHS the ability to automate alerting of detected network intrusion attempts and, when deemed necessary by DHS, to send alerts that do not contain

> the content of communications to the National Security Agency (NSA) so that DHS efforts may be supported by NSA exercising its lawfully authorized missions. … DHS will be able to adapt threat signatures determined by NSA in the course of its foreign intelligence and DoD information assurance missions for use in the EINSTEIN 3 system in support of DHS's federal system security mission. Information sharing on cyber intrusions will be conducted in accordance with the laws and oversight for activities related to homeland security, intelligence, and defense in order to protect the privacy and rights of U.S. citizens.

- In 2010, during the Obama administration, OMB formally delegated to DHS the oversight role FISMA 2002 had given it, but OMB kept its statutory function promulgating NIST-based standards for agencies to follow.
- In 2014, Congress confirmed this division of labor between OMB and DHS, through an updated version of FISMA ("FISMA 2014"). FISMA 2014 also enhanced DHS's authority in a key respect. In addition to having lead responsibility for monitoring agency compliance with OMB rules, DHS now also has the ability to issue "binding operational directives" requiring agencies to take some particular step.
- *The DHS-based organization responsible for both cybersecurity and critical infrastructure protection (encompassing NCCIC and US-CERT, among other things) used to be known by the aggressively non-descript name the National Programs and Policies Directorate (i.e., NPPD). Thanks to new legislation in November 2018, NPPD has a more-fitting name: the Cybersecurity and Infrastructure Security Agency (that is, "CISA"; this is, unfortunately, the same acronym as the 2015 information-sharing and liability-pruning statute we studied previously). Think of CISA as the bureaucratic equivalent of FEMA: a unified, mission-defined component under the overarching management of DHS. This statutory improvement in the bureaucratic optics of the organization does not entail formal change to CISA's authority, yet the move nonetheless is expected by some to increase the stature and influence of CISA (and its Director) in informal ways.*
- **As a matter of institutional design, does this arrangement make sense to you?**
- **Does any of this change your view regarding lessons to be learned from the OPM fiasco?**
- In May 2017, President Trump issued an executive order addressing federal agency cybersecurity, as well as other matters. **Read ONLY section 1 of the order, here.**
  - **Can you describe what, specifically, is new about this (hint: can you explain what "accepted risk" means?)**

C. After the Fail: Managing Consequences

Even if we have strong incentives for potential victims to take protective measures, and even if we impose significant costs on attackers, some successful attacks will occur. What then? Time to manage the consequences.

Breaches come in all shapes and sizes. In most instances, the consequence-management challenge is a matter of concern primarily to the victim entity itself (as well as to those persons whose data may have been exposed). Sometimes, though, a breach has wider significance—perhaps even calling for involvement by the U.S. government.

Our primary aim in this subunit is to consider which situations warrant such involvement, what form might such involvement might take, and how the government has organized itself to answer those questions when particular cases arise. Next, we'll conclude Unit I with a look at a recurring scenario that implicates most if not all of the topics we've considered up to this point in the course: botnets.

17. October 31 Cases of National Significance
18. November 1 same

Most breaches do not implicate the national interest, at least not when considered in isolation. This is certainly true for most private-sector cybersecurity incidents. Put another way, most intrusions do not warrant consideration of whether and how to marshal various instruments of national power in the course of managing the response. But some scenarios *do* warrant exactly that sort of response. Which ones count in this way, who decides, and what follows from such a determination? Our goal is to understand how the U.S. government gradually has developed an approach to answering those questions.

A. Critical Infrastructure

- A good place to begin with this topic is the concept of "critical infrastructure." That phrase captures that idea that our daily lives depend to no small extent on certain particularly-important systems, services, and structures. As DHS has put it: "critical infrastructure provides the essential services that underpin American society and serve as the backbone of our nation's economy, security, and health. We know it as the power we use in our homes, the water we drink, the transportation that moves us, the stores we shop in, and the communication systems we rely on to stay in touch with friends and family." Some of these systems are themselves associated directly with cyberspace (for example, various parts of our communications architecture). But most concern other things such as health care, electricity, sanitation, or transportation.
- There are many potential sources of harm to critical infrastructure. Some of these are unintentional, as with accidents, natural disasters, and simple wear-and-tear accumulating with the passage of time. Others are purposeful, however, as seen with both physical forms of attack and also disruption achieved through cyber means. Our concern, of course, is harm to critical infrastructure achieved via cyber means. More specifically, we want to understand the policy and legal issues associated with minimizing such harm. The ideal way to minimize harm is to prevent it from occurring in the first place. Much of the course up to this point has been concerned with exactly that. Another important part of harm minimization, though, involves optimizing systems for rapid mitigation of harm once it does occur.
- If all critical infrastructure was in the hands of the government, it would be relatively clear how to go about organizing incident response with an eye towards harm minimization. Most critical infrastructure is not in the government's hands, however; for the most part it is owned by private entities. This significantly complicates matters. For systems that are owned by private entities, prevention and mitigation of harm at least in the first instance is the responsibility of the owner. Still, given the high stakes theoretically involved with critical infrastructure, it makes sense that there might also be *some* degree of involvement from *some* government entity. And, as it happens, the federal government for many decades has been developing its procedures for determining its role in such situations.

B. Developing a Critical Infrastructure Strategy During the Obama Years

- Both the Clinton and George W. Bush administrations were aware of this concern, and took a variety of important initial steps in response to it. Having said that, our study of this topic will jump into the sequence of developments circa 2013, with a pair of actions by the Obama administration.
    1. Executive Order 13636 – EO 13636 is not primarily about consequence management (it mostly focuses on encouraging improvements to defense), but it does address the topic to a small extent.
        - *Section 7*: This section directs the National Institute of Standards and Technology ("NIST") to create a "Cybersecurity Framework" meant to help critical infrastructure owners minimize their cyber risk. NIST published the first version of the Framework in February 2014, and then published an updated version in April 2018. The following language from the original 2014 version explains what the Framework does—and does not—aspire to do:

> "The Framework uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity. It supports recurring risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes. Thus, the Framework gives organizations the ability to dynamically select and direct improvement in cybersecurity risk management.... The Framework provides a common language for understanding, managing, and expressing cybersecurity risk both internally and externally. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. … The Core is not a checklist of actions to perform…."

The NIST Framework thus is a template for an organization to engage thoroughly in assessment and management of cybersecurity risk. The graphic below illustrates the range of activities it encompasses in a sequential way. **Which parts, if any, concern consequence management?**

- *Section 8:* Next, **read Section 8(a)** and answer these questions:
  - ***Does* the Executive Order purport to make private sector critical infrastructure owners legally obligated to adopt and adhere to the Cybersecurity Framework?**
  - ***Should* it do so?**
  - **Would it work, legally, to create such an obligation via Executive Order?**
  - **Does the existence of the Framework nonetheless cast a legal shadow of sorts, one that might at least create incentives for CI owners?**
  - Using that same link above, **read Section 8(e). Does this suggest to you another way the government could compel compliance with the NIST Framework?**
  - **Why do you suppose the government did not take a more-prescriptive approach to compelling improvements to private-sector prevention-and-mitigation efforts relating to critical infrastructure?**
- *Sections 9 and 10:* **Read Sections 9 and 10.** Section 9 calls for the government to identify a subset of critical infrastructure entities. **What is the purpose of this subcategory, what is its label, and what is the standard to determine which entities fall within it?** Section 10 directs those federal agencies that happen to have regulatory authority over entities within this subset (for example, the Department of Energy would have authority to regulate a nuclear power plant) to review the sufficiency of their regulations as they might pertain to cybersecurity. Section 10 adds that if an agency concludes it needs

greater regulatory authority in the area of cybersecurity, it should say so. It also requires agencies to report on the possibility of *over*-intrusive regulations. **How might this help both prevention and mitigation?** Finally, notice this from Section 12 of EO 13636: "Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law." **What might explain the inclusion of this language, and does that explanation help you explain in turn why EO 13636 is not more prescriptive?**

2. PPD-21- On the same day that President Obama issued EO 13636, he also issued **Presidential Policy Directive 21** ("PPD-21") (it is available here if you are curious, but you do not need to read it). Among other things, PPD-21 identified 16 critical-infrastructure "sectors" of the American economy, pointing out for each sector which federal agency normally shall play a leading role (the "sector-specific agency," or "SSA"). PPD-21 directs the Secretary of Homeland Security to update the list periodically.
    - PPD-21 borrows from a statute (42 USC 5195c if you are curious) to define "critical infrastructure" to encompass "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." **Are you satisfied by this definition?**
    - Review the current list of **16 sectors** that count as CI. **Do you agree with all the sectors included here? Anything missing?**
    - Just prior to the inauguration of President Trump in January 2017, DHS Secretary Jeh Johnson **added election systems** to the CI list for the first time. **Do you see language in his statement suggesting a felt need to downplay this decision? What might account for that? What factors did Secretary Johnson cite in order to ameliorate possible objections to this step? Does your answer to that question give you reason to doubt whether the critical-infrastructure designation has *enough* significance?**
    - Does Hollywood belong on this list? Recall that North Korea several years ago engaged in a massive hack of Sony Pictures Entertainment, to punish Sony for producing the "comedy" The Interview. Was that best understood as an attack on America's critical infrastructure? Go to the DHS page listing the 16 sectors, and click on the link for the Commercial Facilities sector. From there, navigate to the "Sector-Specific Plan," and use that document to answer this question: **Does DHS think that the Sony Hack was an attack on critical infrastructure?** Next, refer back to PPD-21's definition of critical infrastructure. **Does the Commercial Facilities sector-specific plan seem to stay within the bounds of the PPD-21 definition?**

- Neither EO 13636 nor PPD-21 attempted to spell out how the executive branch should handle coordination, deconfliction, and other matters in the event of a private-sector cybersecurity incident that arguably warranted some form of federal intervention. But a subsequent PPD in 2016—PPD-41, titled "United States Cyber Incident Coordination—took up this task. **Using that link, read the sections noted below in order to answer these questions**:
    - Section II
        - **What is the difference between a "cyber incident" and a "significant cyber incident?"**
        - **Why draw that distinction?**
        - **Ponder the definition of "significant cyber incident." Is it sufficiently clear so as to yield predictable answers as to which incidents fall into that category?**

- Section IV
  - **Can you explain the difference between and among "threat response," "asset response," and "intelligence support/related activities"?**
  - **In practical terms, what specific forms of federal government involvement does Section IV suggest will occur with run-of-the-mill cyber incidents?**
- Section V – This section applies only to "significant cyber incidents."
  - **What is the difference between the Cyber Response Group and the Cyber Unified Coordination Group? Read Section II.A. of a separate document—the "Annex" to PPD-41—to understand who sits on the CRG and what it should do. Then read Section II.B of the Annex to understand more about the Cyber UCG concept.**
  - **Why do we need either of these in relation to "significant cyber incidents," but not run-of-the-mill "cyber incidents"?**
  - **In Section V(c), certain responsibilities are placed on the FBI (in coordination with the National Cyber Investigative Joint Task Force organization, which FBI leads), DHS (in the form of CISA's NCCIC unit), and the Office of the Director of National Intelligence (through its CTIIC). How if at all is this different from what would occur if an event was merely a "cyber incident"?**

- The National Cyber Incident Response Plan—The last part of the Annex to PPD-41 directed DHS to work with others to create a "national cyber incident response plan" within six months. In December 2016, DHS accordingly published **The National Cyber Incident Response Plan.** The full version is available here, but *don't read the whole thing (unless you want to!).* I'm only interested in having you **read the section on "Operational Coordination During a Significant Cyber Incident," which starts on p. 29 and ends on p. 35, plus Annex B on p.38**.
  - The NCIRP sheds additional light on when an incident counts as "significant." **How so, and did you find this useful?**
  - You have seen how both PPD-41 and the NCIRP empower certain entities to take a lead role in terms of threat, asset, and intelligence response. **Would you add or subtract anything from this arrangement, and if so would you make that change as to all significant cyber incidents or only upon satisfaction of certain conditions?** That's another way of asking: **Do we need further gradations of severity in order to enable different default rules for lead agency responsibility and mandatory decision-making and coordinating processes? Or is this the sort of question that does not—and perhaps should not—be reduced to clear rules in advance?**

C. The 2017 Executive Order from the Trump Administration

- In May 2017, President Trump issued **Executive Order 13800 ("Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure")**. In an earlier class we read portions of it dealing with the task of improving the security of federal systems. Now we look at what it has to say about protection of CI. **Read the following subparts of Section 2 of EO 13800,** and consider the following questions:
  - **Section 2(b)**—This subsection gave DHS six months to investigate the prospects for the federal government to do more in relation to protecting the CI entities identified under "Section 9" of EO 13636 (Feb. 2013) (see above to remind yourself what that means). **What do you suppose the drafters had in mind here as a possibility, and what obstacles might arise if the government pursues that course?**
  - **Section 2(c)**—This subsection calls for study of "market transparency of cybersecurity risk management practices by" CI entities, especially the public-traded ones. **What is this about, and how might pressure in this area help spur better security practices?**

D. Why not just have government directly prevent and mitigate attacks on these systems?

- Have you noticed that none of the documents reviewed above has attempted to address cyber threats to critical infrastructure by having a government entity—the NSA, CYBERCOM, etc.—actually take direct responsibility for monitoring networks and performing security functions directly on behalf of private entities. **List the pros and cons of empowering NSA or other government entities to take on such a role.**
- Note that there is no reason to think DOD affirmatively seeks such a mission. Consider this excerpt from the written testimony of a Defense Department official, before the Senate Armed Services Committee, in October 2017:

> STATEMENT OF MR. KENNETH RAPUANO
> ASSISTANT SEC. OF DEF. FOR HOMELAND DEFENSE & GLOBAL SECURITY
>
> TESTIMONY BEFORE THE SENATE ARMED SERVICES COMMITTEE OCTOBER 19, 2017
>
> …Although DoD has built capacity and unique capabilities, for a number of reasons, I would caution against ending the current framework and against reassigning more responsibility for incident response to the Department of Defense.
>
> First, DoD's primary mission is to provide the military forces needed to deter war and to be prepared to defend the country should deterrence fail, which requires us to be prepared at all times to do so. DoD is the only department or agency charged with this mission, and success in this requires the Department's complete focus. In this case, any significant realignment of roles and responsibilities will have opportunity costs, including absorptive capacity to build mission capability in a new area, especially ones that could distract the Department from its core warfighting missions.
>
> Second, the United States has a long normative and legal tradition limiting the role of the military in domestic affairs. This strict separation of the civilian and the military is one of the hallmarks of our democracy and was established to protect its institutions. Designating DoD as the lead for the domestic cyber mission risks upsetting this traditional civil-military balance.
>
> Third, a primary civil reliance on DoD in the steady-state would result in increased demands that could not be met without significant changes in resource allocation. We would expect even greater demand in a conflict scenario, when there might be a natural tension in the need to preserve DoD mission capabilities and requests for support to civilian agencies. Even with such a change in resource allocation, the addition of a new mission would likely detract from the focus on and readiness for the warfighting mission.
>
> Finally, putting DoD in a lead role for cyber incidents creates an exception to accepted domestic response practice in all other domains, which would disrupt our efforts to establish and maintain unity of effort. Civilian agencies have the lead responsibility for domestic emergency response efforts; this should not be different for cyber incidents. The Federal Government should maintain a common approach to all national emergencies, whether they are natural disasters or cyberattacks.

- Is there a "third way" alternative? Consider this concept, advanced by then-Deputy Secretary of Defense William Lynn in a speech in 2010:

> "Years of concerted investments on the military side have placed critical cyber capabilities within the Defense Department and National Security Agency. We are already using our technical capabilities to support DHS in developing the Einstein 2 and 3 programs to protect government networks. We need to think imaginatively about how this technology can also help secure a space on the Internet for critical government and commercial applications.
>
> For the .com world, could we create a secure architecture for that lets private parties opt-in to the protections afforded by active defenses? In this way protection would be voluntary. Operators of critical infrastructure could opt-in to a government-sponsored security regime. Individual users who do not want to enroll could stay in the "wild wild West" of the unprotected Internet. This type of secure.com approach could build on the collaboration between DoD and the defense industry. It could offer an important gateway to ensure our nation's critical infrastructure is protected from cyber attacks."

  - **What are the pros and cons of this bifurcated model?**

II. THE OFFENSIVE PERSPECTIVE

We've been defense-focused for many weeks now. That is, we've surveyed the institutions, laws, and policies intended to deter, prevent, and mitigate the consequences of unauthorized access. For better or worse, however, defense is not always the overarching policy goal. In the U.S. system, some institutions, laws, and policies promote (or at least tolerate) *offense*—that is, efforts to penetrate or interfere with a system without its owners authorization (or, perhaps, awareness). For the sake of convenience, we might call this lawful-but-unauthorized access (meaning lawful from a U.S. perspective; needless to say, such activity may well violate the laws of other countries when they occur overseas).

You will note immediately, I hope, that the very idea that this category exists is in considerable tension with the policy goals advanced by, well, pretty much everything we studied in Unit I. Why, then, should there even be such a category? We will explore that question across several contexts.

To a substantial extent, lawful-but-unauthorized access frameworks rest on the counterintuitive claim that it can, in the right circumstances, promote security. We see this, for example, in the arguments advanced by those who advocate empowering the private sector to respond to an attack with self-help measures that will have effect outside their own networks (that is, effects on the attacker's network, or more likely effects on intermediary networks through which an attack was routed). That's the "hack back" scenario, and we will focus on it first.

But the case for lawful-but-unauthorized access does not have to rest entirely on that ground. In most cases, in fact, lawful-but-unauthorized access is intended to promote other values. We see this with law enforcement investigations, collection of foreign intelligence (that is, espionage), promotion of U.S. foreign policy or military goals via covert action, and military action both above and below the threshold of armed conflict. We will survey each of

those scenarios, with an emphasis on the key institutions, policy conflicts, and legal framworks.

19. November 7 – Should We Allow the Private Sector to Hack Back?

Are there circumstances in which we want someone in the private sector to be able to access another's system without their permission? We just completed a long unit focused on how the United States discourages that sort of thing, so the idea of encouraging it at first blush seems jarring. As we will see this, however, there is a context in which some believe that the rules currently allow—or, if not, should be *changed* to allow—precisely this result.

A. Why does this question arise? A hypothetical scenario to give us a frame of reference

- Assume an OPM-like scenario involving a private sector entity, which we will call Company X. The Chief Information Security Officer ("CISO") of Company X has just notified the CEO and the General Counsel that someone has gained unauthorized access to the company's network, has accessed sensitive files, has exfiltrated copies of some of these files to some external server already, and at this moment appears to be exploring for more such files.
- You are the CEO. The CISO tells you that she has done some analysis, and is confident about a few things. First, she has determined the IP address of the server where the attacker appears to have stored the exfiltrated files at least initially. She says that her team very likely could cook up some malware of their own in order to access that server, and once inside to locate and delete any of the company's files found there. It should also be possible to determine who controls the server, including the possibility that it is some innocent third-party whose own machine was compromised by the actual attacker in order to serve this staging function. In the latter case, the CISO says, it might also be possible to locate the server issuing orders to the compromised intermediate server, and so on until the identity of the attacker might become clear. The CISO is ready to make some or all of these attempts right now.
  - **From a policy perspective, why might it be good to authorize the CISO to carry out some or all of these steps?**
  - **Why might it be bad?**
  - Remember the Computer Fraud and Abuse Act.
  - **Do any of these proposed actions potentially violate the CFAA?**
  - **Which specific section(s) of 18 USC 1030(a) might be violated?**
  - **If Company X cannot or should not take these steps, are there other entities that might do so—and are there obstacles to them doing so effectively?**
- Second, the CISO has identified the malware on the company's system that gave the attacker initial access to the company's system. Predictably, she says, it got there via an email phishing attack. You ask who was dumb enough to click on some infected link in an email. She coughs and looks at you uncomfortably, mumbling something about how this sort of thing could happen to anyone. You realize it was you… Happily, the CISO quickly changes the subject, explaining that she can easily remove the malware now.
  - **Pros and cons of acting to remove the malware right now?** (remember the OPM version of that issue)
  - **Does removing the malware create exposure under the CFAA?**
- The CISO says there is another option: She could lay a trap for the intruder, generating a file designed to be attractive to the attacker but loaded with a hidden beacon. A "beacon," in this context, is a program that will make periodic attempts to contact a control server in order to report on the current location of the file in which it is embedded. The CISO explains that this would be the digital equivalent of a GPS tracker hidden in a bag of cash stolen from a bank.
  - **Wisdom of this step?**

- ***o*** **Legality under the CFAA?**
- Now assume that the company decides to pursue an aggressive option, tricking the intruder into exfiltrating a file that, when opened, will function as ransomware—*i.e.,* encrypting as much of the system as possible while indicating to the system operator whom to contact or what other steps to take in order to recover access to their data.
  - **o** **Wisdom of this step?**
  - ***o*** **Legality under the CFAA?**

B. Statutory Reform—CISA 2015

- If you are inclined to think that certain forms of hack back may be desirable, but not actually allowed under CFAA (or, at least, not sufficiently clearly allowed), you might then consider the possibility of a statutory reform. And, indeed, some have pursued just that.
- First, let's look back to a statute we previously studied in relation to information sharing. Remember CISA, the 2015 Cybersecurity Information Sharing Act? **Read Section 104(a),** which appears below in full:

(a) AUTHORIZATION FOR MONITORING.—

1. IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, monitor—

   A. an information system of such private entity;

   B. an information system of another non-Federal entity, upon the authorization and written consent of such other entity;

   C. an information system of a Federal entity, upon the authorization and written consent of an authorized representative of the Federal entity; and (D) information that is stored on, processed by, or transiting an information system monitored by the private entity under this paragraph.

2. CONSTRUCTION.—Nothing in this subsection shall be construed—

   A. to authorize the monitoring of an information system, or the use of any information obtained through such monitoring, other than as provided in this title; or

   B. to limit otherwise lawful activity.

- Consider how this statute might apply to each of the measures recommended by the CISO in the hypothetical case of Company X, above.
  - **o** **Does Section 104(a)(1) make lawful anything that otherwise would be unlawful?**

Next consider Section 104*(b)* of CISA, which speaks of certain activities that count as "defensive measures" as defined in CISA. Before looking at the text of 104(b), in fact, we should pause to look at the statute's definition of "defensive measures." Here it is, from Section 102(7):

7. DEFENSIVE MEASURE.—

A. IN GENERAL.—Except as provided in subparagraph (B), the term "defensive measure" means an action, device, procedure, signature, technique, or other measure applied to an information system or information that is stored on, processed by, or transiting an information system that detects, prevents, or mitigates a known or suspected cybersecurity threat or security vulnerability.

B. EXCLUSION.—The term "defensive measure" does not include a measure that destroys, renders unusable, provides unauthorized access to, or substantially harms an information system or information stored on, processed by, or transiting such information system not owned by—

i. the private entity operating the measure; or

ii. another entity or Federal entity that is authorized to provide consent and has provided consent to that private entity for operation of such measure.

- Now, on to Section 104(b) itself. It reads in full:

(b) AUTHORIZATION FOR OPERATION OF DEFENSIVE MEASURES.—

1. IN GENERAL.—Notwithstanding any other provision of law, a private entity may, for cybersecurity purposes, operate a defensive measure that is applied to—

A. an information system of such private entity in order to protect the rights or property of the private entity;

B. an information system of another non-Federal entity upon written consent of such entity for operation of such defensive measure to protect the rights or property of such entity; and

C. an information system of a Federal entity upon written consent of an authorized representative of such Federal entity for operation of such defensive measure to protect the rights or property of the Federal Government.

2. CONSTRUCTION.—Nothing in this subsection shall be construed—

A. to authorize the use of a defensive measure other than as provided in this subsection; or

B. to limit otherwise lawful activity.

- Taking both Section 102(7) and 104(b) together, let's consider how they might apply to our hypothetical CISO suggestions:
  - **Does this change the legality of any of the hypothetical steps?**

C. Statutory Reform: The "AC/DC" Act?

- Not surprisingly, CISA was not the last word on a possible statutory change relating to hackback. Last year, two members of Congress introduced a bipartisan bill called the Active Cyber Defense Certainty Act (that's right, it's the AC/DC Act; insert puns here!). **Read it here, focusing on Sections 3 through 6**. In class, we will do a close review of these sections, with the goal of identifying what they seek to accomplish, whether they succeed, and whether the balance of costs and benefits seems worthwhile.
- Note that the bill has received a frosty reception in some quarters, and has not yet been enacted.

20. November 8 – Hacker Cops? Network Investigative Techniques
21. November 15 - same

Are there circumstances in which we want law enforcement officials to have the option of using unauthorized access to gather evidence? That is, do we want there to be situations in which law enforcement by law has authority to circumvent the security of a machine or device, without the owner/controller's knowledge or permission, in order to gather evidence of crime? And is this already possible, at least to some extent, under current law and policy?

There are many variables that might impact your analysis of this issue. For example: Is the system in question (that is, the one to be breached) physically located in America? Is the target of the investigation, or in any event the person whose data is in issue, a US person with Fourth Amendment rights? How exactly will the breach be effectuated? Will the breach have effects other than mere acquisition of information? Does the operation run the risk of diplomatic repercussions, and if so of what kind and severity? Who will decide whether to do it, who will actually do it, and what oversight if any might there be?

A. Network Investigative Techniques: Introduction to NITs and the Fourth Amendment

- **Read this article from Kim Zetter at Wired** for an overview of law enforcement hacking—that is, the use of what the FBI would call a "Network Investigative Technique," or "NIT."
  - **What are the potential policy benefits of allowing law enforcement to obtain evidence via hacking, and what are the potential costs?**
  - **Does your assessment of the policy pros and cons change if we assume for the sake of argument that the government has a search warrant (or, conversely, if we assume that it does not)?** Context for those not already familiar with how search warrants work: The Fourth Amendment to the Constitution of the United States provides that an investigative measure that qualifies as a "search" must be "reasonable," and also that no warrant can be issued by a judge unless the government shows that there is "probable cause" to believe that a crime

has been committed and that the proposed investigation will yield evidence or fruits of that crime. Generalizing a bit, the courts have interpreted all this to mean that the government normally must have a warrant—and must stay within its terms when conducting the search—or else the fruits of the search will be suppressed (that is, excluded from admission at trial). Of course, that puts a lot of weight on the question of what counts as a "search" triggering this requirement. Since 1967, the test has been whether the person has a "reasonable expectation of privacy" in the thing or location being searched (with the reasonableness of that expectation being both a subjective and an objective inquiry).

- As a general proposition, people have a reasonable expectation of privacy in the data they locally-store on their phones, pads, and laptops. But then again, we increasingly don't store data locally on the good ol' C: drive. Or at least we don't exclusively store it there. More and more, we rely on cloud services that centrally store data on the servers of the company in question and then download files to the local device as needed. This, it turns out, may have significant constitutional implications. The Supreme Court has long held that when you have sensitive information but it is in the hands of a third party—like, say, your bank's possession of records about your financial transactions—you have effectively waived your claim to have a reasonable expectation of privacy. That rule—the so-called "Third Party Doctrine"—has been under pressure in recent years thanks to the evolution of communication and data storage technologies, and a few months ago the Supreme Court in a case called *Carpenter* held that the Third Party Doctrine should not apply to the specific situation in which the government sought seven days' history of the location data that a cell-phone service provider possessed about a customer's phone thanks to the fact that our phones are constantly connecting to the nearest tower. The Court explained that a combination of factors—including the comprehensiveness, depth, breadth, and unavoidability of this particular sort of data—made it different in kind from the analog-world scenarios that gave birth to the Third Party Doctrine originally. The Court was at pains to state that it was not overturning existing applications of the Third Party Doctrine, however. **What does this have to do with NITs?**

- Another complication arises when data is stored outside the United States. The Fourth Amendment clearly protects the reasonable expectations of privacy of US persons and others within the United States, but under current caselaw it does *not* protect the privacy interests of non-US persons outside the United States. **What does this have to do with NITs?**

- The first example of an FBI investigative technique mentioned in the article is "Carnivore." That system was more in the nature of a wiretap, however, than a technical hack to circumvent information security measures. Still, the Carnivore story is a useful setup to explain the government's later interest in "keylogger" software. **What is a "keylogger" and what technical problem did that approach solve?**

- The Scarfo investigation led to a complaint by a Justice Department official suggesting that FBI had "risked a classified technique on an unworth[y] target." **What harm could follow from using the keylogger at issue there?**

- **What was different about Magic Lantern as compared to the Scarfo keylogger?**
- The next example in the article—CIPAV—concludes with the notion that Justice Department officials worried that excessive use of the NIT increased the "risk of suppression." **Does that mean something improper was going on? What could CIPAV do and when is that desirable?**
- The Watering Hole Strategy: **What is a "watering hole" in this context, and why might this approach be useful for NIT delivery?**
- The article concludes with a section subtitled "Big Questions Remain." **Read carefully, and decide which of these questions seem most significant to you.**

B. NITs, International Relations, and International Law

- Sometimes NITs target systems that are located overseas and thus give rise to serious international relations and legal complications. **Read this short paper from Orin Kerr and Sean Murphy (responding to concerns from Ahmed Ghappour)** exploring some of the resulting issues.
  - **What had Professor Ghappour argued regarding the implications of international NITs for international relations?**
  - **How did Professors Kerr and Murphy respond?**
  - **Why might one think that an international NIT violates international law?**
  - **Why did Kerr and Murphy reject that view?**
  - **What if anything do we learn here regarding the internal system of management and oversight regarding the use of international NITs?**

C. The Disclose-or-Dismiss Dilemma

- As we saw above, the Justice Department and FBI worry about maintaining the secrecy of how some such tools work. **Read this Lawfare piece by Susan Hennessey and Nicholas Weaver** in order to better understand how NITs function and why prosecutions can result in dilemmas pitting the interests of preserving secrecy against those of securing convictions.
  - **Can you explain this dilemma?**

D. The Going Dark Debate: What Has This Got to Do With NITs?

- That same Lawfare piece notes the connection between the idea of law enforcement hacking and the government's oft-stated fear that the diffusion of strong encryption can and will produced a "going dark" situation in which the government has a warrant (or other lawful authority) to access a system (a laptop, a phone, a message in transit) but neither it nor the company that made the system can decrypt the information therein.

- **To understand this issue better, read pages 1-15** (as numbered in the original text of the document, not just counting from the start of the pdf) **of the "Don't Panic" report** issued by the Berkman Center at Harvard. **Then read this essay from Susan**

Hennessey for Brookings (titled "Lawful hacking and the case for a strategic approach to 'Going Dark'").

- **What are the policy concerns that motivate the FBI here?**
- **What are the offsetting policy concerns?**
- **What factors might make the situation worse for the FBI over time, and what factors might make it better?**
- **What role does the "lawful hacking" idea play in addressing "going dark," and is it necessarily cost-free to encourage resort to that solution?**
- **Are state/local law enforcement entities similarly-situated to the FBI with respect to these debates?**

22. November 28 Spy games: Hacking as Espionage & Covert Action

A. What Do We Mean By "Intelligence Activities"?

- In prior classes, we have repeatedly discussed two categories of government activity (espionage and covert action) that usually are conducted by intelligence agencies and thus usually fall under the general heading of "intelligence activities." Now we are going to revisit those concepts in a more systematic and contextualized way, using that larger label—i.e., "intelligence activities"—to frame our study.
- Much like "active defense," the phrase "intelligence activities" means different things to different people, and you need to be on guard against miscommunication as a result. That said: for our purposes, "intelligence activities" is an umbrella phrase meant to encompass no more and no less than the various categories of activity that an intelligence agency might engage in. The leading examples of those categories, as commonly understood in the U.S. context, include:

  1. Analysis – "Analysis" refers to the process in which experts apply their knowledge to information that has been gathered from various sources (open sources, human sources, signals intelligence, and so forth) in order to produce insights that then can inform the decisions and behaviors of a particular agency's various "customers" (such as the President, military commanders, diplomats, trade negotiators, etc.). Put another way, analysis is a scholarly process that is much more than just the circulation of raw information. The goal is to use expertise to convert raw information into "intelligence products." The President's Daily Brief ("PDB") produced by the ODNI is a particularly-famous example.

  2. Collection – Where do analysts get the information that helps them produce products? That information has to be *collected* in the first instance. Some (but not all) collection takes the form of "espionage"—i.e., surreptitious, unauthorized acquisition of information. Espionage might take the form of hacking, but older and still-relevant options include inducement of a human source (with the inducement typically involving one of more of: money, ideology, coercion, or ego), interception of radio or other electromagnetic spectrum signals, satellite or aerial imagery, physical break-ins, and so forth. Note, though, that there is plenty of important information out there in "open sources," too (more so in recent years thanks first to the Internet and now especially to social media). Collection from such open sources is an increasingly-important task for intelligence agencies. Note that it also has something

of a levelling effect, as open-source collection for the most part is comparatively easy for non-state actors and less-resourced government agencies to perform.

3. Covert Action – Covert action is an American term-of-art used for legal and policy purposes to categorize an activity that the government intends to have an actual effect (as opposed to merely collecting information) and where the sponsoring role of the government in causing that effect is not meant to be apparent or acknowledged. In short, covert action seeks to alter real-world circumstances in some fashion, without the government taking public responsibility for doing so. Critically, this category might involve all sorts of different conduct, ranging from the innocuous to the dramatic. For example, a covert action program might involve a modest, brief attempt to influence foreign opinions on some minor point, but then again it also might involve a massive and sustained campaign of sophisticated efforts to drive foreign opinions on a critical matter such as an election. Similarly, it might involve a modest effort to create physical problems in the development process for a foreign government's weapons program, or it might even entail the use of actual force—perhaps even lethal force—towards that end. Obviously, covert action in general presents a variety of legal, policy, and moral issues, and those issues sometimes are heightened by the particular details of the covert action in question (such as election meddling or the use of lethal force).

- Analysis plays an important role, obviously. But for purposes of Unit II—with our emphasis on situations in which we encourage unauthorized access to computer systems—it is espionage and covert action that concern us.

<u>B. Ambiguity about Categorization</u>

- Recall a critical point we have emphasized in prior classes: these categories are conceptually distinct in theory, yes, but the distinction is not always present or discernible in practice. First, it is possible for particular scenarios to incorporate elements of more than one category at the same time. Second, some operations entail the option of pivoting from one purpose (say collection) to another (covert action), and thus proper categorization might be clear at one point but can then change. Third, and relatedly, it is possible that the right categorization just is not clear to an outsider with only limited factual understanding.
- Consider this example: A CIA case officer cultivates a relationship with an Iranian scientist involved in Iran's nuclear program. The scientist is in a position both to share secrets and to cause practical problems for the nuclear program by interfering with equipment.
  - **Should we categorize the recruitment as collection or covert action?**
  - Assume that Iranian counterintelligence officials suspect something is afoot. **Will they necessarily come to the same conclusion?**
  - **What if we are instead dealing with an intelligence activity in which a U.S. agency uses an exploit to gain access to a computer associated with Iran's nuclear enrichment program?**

<u>C. Meet the U.S. Intelligence Community ("IC") and Some of Its Key Components</u>

- The phrase "Intelligence Community," often abbreviated as "the IC" (pronounced eye-see), is used in the United States to refer to the collection of federal agencies that engage in intelligence activities. Here's a thumbnail sketch of some of the key players for our purposes:
- First, the big picture: the IC consists of *seventeen* different entities. Eight of them are part of the Defense Department (including, most notably for our purposes, the National Security Agency), and thus come within the budget, policy, and personnel domain of the Secretary of Defense. Seven others are part of the Departments of Justice, State, Treasury, and Homeland Security. Only two stand independent: the CIA, and the Office of the Director of National Intelligence (ODNI).

- ODNI was created in 2004 with the goal of providing IC-wide coordination and services, and thus the Director of National Intelligence ("DNI") to some extent function as the head of the IC. The DNI's control over other IC members is limited both formally and functionally, however. One might say that the DNI combines with the Director of the CIA and the Secretary of Defense (or, perhaps more accurately, the Under Secretary of Defense for Intelligence) to form a sort of informal triumvirate of senior-most intelligence officials in the U.S. government.
- In various ways, all seventeen components of the IC are relevant in relation to cybersecurity, for most of them engage in analysis and analysis is an important part of the defensive mission we examined in Unit I. But as noted above, our concern in Unit II is with situations in which the United States government encourages unauthorized access, and so we will focus on collection and covert action here.
    - That said, it is worth pausing to introduce a relatively-new part of ODNI that plays an important role in analysis and interagency coordination from a defensive perspective. In February 2015, possibly in response to a White House perception that the IC's members were not sufficiently coordinated in determining who carried out the attack on Sony that ultimately was attributed to North Korean, President Obama ordered the Office of the Director of National Intelligence to establish the **Cyber Threat Intelligence Integration Center ("CTIIC").** CTIIC was directed to "provide integrated all-source analysis of intelligence related to foreign cyber threats or related to cyber incidents affecting U.S. national interests," serving as a sort of interagency hub for sharing and analyzing such information. **Can you articulate how this mission differs from that of NCCIC, US-CERT, and FBI Cyber Division?**
- **The National Security Agency ("NSA"):** NSA is part of the Department of Defense, and has a complex set of missions that include collection and analysis (but not covert action). Most obviously, it is the lead agency for collecting foreign intelligence through electronic means in order to suit the needs of national customers like the President. Less obviously, it also collects to address the needs of military customers, including collection in support of ongoing combat operations. Further, NSA has a parallel defensive mission (as we have noted previously when discussing the protection of government networks). NSA also performs analysis of the information it collects. And, finally, NSA performs advanced research and development relating to various aspects of communications security (including, famously, cryptography). Note that the Director of the NSA also serves, simultaneously, as the commander of United States Cyber Command ("CYBERCOM), which we will study in our next session). This arrangement is called "the dual hat."
- **The Central Intelligence Agency ("CIA"):** CIA is an independent federal agency that performs all three intelligence activities described above. It is the premier agency for conducting collection through human sources, though its collection methods are not limited to that approach. CIA also is America's lead agency for conducting covert action.
- **The Federal Bureau of Investigation ("FBI"):** The FBI is, first and foremost, a law enforcement agency, and we already have explored FBI's use of Network Investigative Techniques (NITs) in the law enforcement investigative setting. But FBI is not just a law enforcement agency. In contrast to the British model, for example, FBI has a dual role in which it also serves as lead agency for collecting intelligence on foreign threats within the United States (that is, "foreign intelligence").

D. The Domestic Legal Framework for Collection and Covert Action

- Over the past five decades, the United States has developed a complex legal framework relating to both collection and covert action activities. A full study of that framework is beyond the scope of this course (my spring course on the Law of the Intelligence Community course covers it). There are some highlights that we should address, however.

- Like most legal frameworks pertaining to government activity, the legal architecture for intelligence activities addresses three types of question: Which agencies have affirmative authority to engage in certain kinds of activity? What process must be followed in order for an otherwise-authorized agency to use its authority? And what substantive limits does the law place on the resulting activity?

  1. Authority - What is the affirmative legal authority for particular agencies to conduct particular intelligence activities (such as hacking to further a collection or covert action program) in the first place?

  a. Collection: There is no serious dispute about the affirmative authority of certain IC members to engage in collection. Take the CIA: Congress has expressly authorized it to "collect intelligence through human sources and by other appropriate means," 50 USC 3036(d)(1), and has appropriated considerable sums for this purpose since the mid-20th century. Even if this were not the case, the executive branch would assert inherent authority to engage in foreign intelligence collection under Article II of the Constitution, citing the president's duties in relation to both foreign affairs and national defense. Note that this is quite different—and much less controversial—than asserting inherent authority also to override a statutory constraint. It is simply a claim that Congress's affirmative permission is not needed in order to engage in foreign intelligence collection (though Congress's *money* may well be needed!). As for NSA? The situation there is somewhat different, for there is no comparably-clear statutory statement spelling out NSA's various missions. There is a comparable history of Congressional funding and oversight, however, not to mention a deep history (for NSA is the institutional successor to Army and Navy entities performing similar functions in the first half of the 20th century) of presidents asserting authority to order the military to conduct this mission. The interesting questions about CIA and NSA collection, as we shall see, tend to concern not authorization as such, but rather the rules of process and substantive constraints spelled out below.

  b. Covert action: Covert action once was different. That is, there used to be a significant debate regarding whether the CIA in particular really had statutory authorization to engage in such activity. Defenders of CIA's covert action role in the past would point either to the president's inherent Article II authorities or else the euphemistic language in the National Security Act of 1947 which referred to CIA conducting "such other functions and duties relating to intelligence" as might be directed. That debate is no longer live, however. Beginning in the early 1970s, Congress began imposing process and substantive rules relating to covert action, and in doing so removed any doubt that such activity was in fact authorized by Congress (so long as it complied with the new rules, which we will explore below).

  2. Process – Congress has passed a number of statutes regulating the process of engaging in both collection and covert action. Some of these rules control the *ex ante* process of deciding to engage in some particular activity (for example, must the executive branch obtain approval from a judge, or must some particular executive branch official approve?), while others involve *ex post* oversight (in the form of reporting to Congress).

  a. Collection*:* With respect to collection, the interesting issue is whether and when the government must obtain *judicial* approval for something it seeks to do. This is an immensely complex topic in general, and it is hard to talk about its application to hacking without going too far down a rabbithole. For our

purposes, though, the following sketch will suffice. First, bear in mind that the scenario we have in mind is one in which a U.S. intelligence agency might seek to gain unauthorized access to a computer in order to engage in collection. If this scenario comes up outside the United States, with non-U.S. persons as the target of the collection, then under current law there is no obligation (under either the Fourth Amendment or a statute) to obtain judicial permission. If, on the other hand, the target is a U.S. person or the collection activity will take place within the United States, it becomes much more complicated. If the aim is to engage in electronic surveillance of the target's communications, a court order almost certainly is required under the 1978 Foreign Intelligence Surveillance Act. In practical terms, that means asking the Justice Department's National Security Division to go to the Foreign Intelligence Surveillance Court (consisting of regular federal judges holding an additional appointment for this purpose) to authorize the surveillance based on a showing that there is probable cause to believe the target is a foreign power or agent of a foreign power.

- **What are the pros and cons of judicial involvement in that situation?**
- **What are the pros and cons of *not* having judicial involvement with overseas collection on foreign targets?**

Note that, regardless of whether court involvement is required *ex ante*, a separate statute (two of them, actually) requires the IC to keep the House and Senate Intelligence Committees "fully and currently informed" of intelligence activities. See 50 USC 3091, 3092.

b. Covert action: There is a simpler framework that governs the decision to engage in covert action, and it does not concern courts. Instead, it is a matter of requiring particular executive branch officials to sign-off on covert action proposals. Title 50 of the US Code requires that any activity counting as a covert action must be approved by the President in writing. We call that the requirement of a presidential "finding." This has been the rule since the early 1970s. Prior to that time, there were no statutes attempting to regulate the covert action decision-making process, and presidents were under no obligation to commit in writing to the approval of covert action programs.

- **What benefits flow from this, and what costs?** Think about it from the point of view of the president. **If you had to sign such a finding, would you insist on certain internal procedures before you had to make that decision?**

As with collection, there also is a requirement that the executive branch share findings with the House and Senate Intelligence Committees (though with covert action, that sharing can be limited to certain leadership figures).

- **Does the obligation to "report" the finding to the intelligence committees accentuate the pros and cons you identified above, or reveal any new ones?**

Critically, Congress for better or worse has elected to add several statutory exemptions to the definition of covert action, removing the obligation to comply with the presidential finding requirement and the notification to the intelligence committees in certain situations notwithstanding that these situations involve an intent to influence events overseas without the U.S. government's role being apparent or acknowledged. Most significantly, it has stated that the covert action statutory process rules do not apply if the activity count as a "traditional…military activity" (often referred to as "TMA"). An operation that qualifies as TMA therefore is not a "Title 50 covert action" after all, but instead a "Title 10 activity" (Title 10 being a part of the U.S. Code that addresses only the Defense Department). Alas, there is a long history of

confusion surrounding the definition of TMA (and, hence, a long history of confusion about the line between Title 10 and Title 50 operations), and as of a few months ago some new legislation speaking to this question in specific relation to hacking.

- Simplifying things a bit, the long-standing debate involves at least two camps. One takes a literal approach. On that view, an operation can count as TMA (and thus escape the covert action rules) only where it not only is to be performed by the military but also is of a kind (or at least quite analogous to a kind) traditionally performed by the military.
- The other camp focuses (more accurately, in my view) on the detailed legislative history of the TMA statutory exemption. That history describes a broader exemption that eschews historical comparisons and instead simply asks (1) whether the operation in question is to be commanded and conducted by military personnel, and (2) whether it relates either to an ongoing armed conflict or to a circumstance for which operational military planning has taken place (which is a *very* wide set of circumstances).
- **Can you see (and explain) why this difference of legal interpretation might matter for an otherwise-covert cyber operation?**
- That debate continues unaltered in relation to most situations involving military activity that smacks of covert action, but recently Congress intervened on this subject specifically in order to reduce uncertainty about when a military-conducted cyber operation can qualify for the TMA exception. *We will explore that plot twist in detail in our next assignment, which focuses on the role of US Cyber Command.*

3. Substantive legal limits: In addition to allocating affirmative authority to perform certain actions and to requiring certain decisionmaking and reporting procedures, Congress also can regulate intelligence activities by placing certain actions off limits. That is, Congress could specify certain things that NSA, CIA, and other intelligence agencies simply may not do when collecting or engaging in covert action. For example, it could ban certain more extreme forms of covert action, such as the use of lethal force. Or it could produce a targeted ban on actions in certain places or for certain purposes. And so forth. So, what has Congress actually done?

a. Collection – Whereas Congress has passed many rules relating to the decisionmaking and reporting processes for collection (though only where there is a U.S. person target or collection occurs within the United States), it has said little about substantive limitations on collection. The one clear counterexample is found in FISA, which specifies that a FISA judge may not conclude that a U.S. person is an agent of a foreign power (and thus a proper surveillance target) based "solely" on First Amendment-protected activities. 50 USC 1805(a)2)(A).

b. Covert action - There are a few substantive rules set forth in 50 U.S.C. 3093. First, section 3093**(f)** provides that covert action cannot be used with intent "to influence United States political processes, public opinion, policies, or media."

- Consider the following hypothetical situation: A president wants CIA to conduct a covert action that would include efforts to hack the personal email and social media accounts of various prominent foreign officials, then use the information obtained to plant stories in that country's media in hopes of impacting an upcoming election. **Would this be barred by section 3093(f)?**

Another part of Section 3093—3093**(a)(5)**—states that the president's finding authorizing a covert action "may not authorize any action that would violate the Constitution or any statute of the United States."

- Refer back to the hypothetical situation in the previous question. **Would section 3093(a)(5) prohibit that activity?**
- The proposed activity certainly would violate the criminal laws of the foreign state in question. **Does 3093(a)(5) therefore bar the activity? What other considerations might come into play, besides legality as such?**
- Assume for the sake of argument that the proposed covert action would violate an international treaty or customary international law. **Does 3093(a)(5) thus prohibit it? What other considerations might come into play, besides legality as such?** Note: we will explore international law as it relates to nation-state hacking in the class-after-next.
- Change the hypothetical such that a US agency will hack into foreign systems to acquire information, but nothing else will occur except the use of this information for analysis purposes. **Does this change your analysis to the questions above?**
- Change the hypothetical again, such that a US agency will hack into a foreign system for purposes to be determined later as circumstances dictate. **What complication does this introduce, and does it alter any of your answers?**

23. November 29 – Cyber War? Introduction to Cybercom

In this class and the next, our focus switches to the U.S. military.

A. Categories of Military Activity in the Cyber Domain

At the risk of oversimplifying things, we might say that the military engages in three categories of activity in the cyber domain:

1. ISR – Not surprisingly, the U.S. military engages in information collection and analysis on matters relevant to its missions and operations. Rather than calling that "collection" or "espionage," however, the military traditionally calls this function "ISR" (an acronym that stands for "Intelligence, Surveillance, and Reconnaissance"). ISR always has been an important military function both in war and in peace, taking various forms ranging from cavalry scouts and foot patrols to aerial photography and radio intercepts. The cyber domain, from this perspective, is merely a (relatively) new environment in which ISR might occur.

2. Network defense - The military of course defends its own communication networks. Those networks are known, collectively, as the Department of Defense Information Network, or "DODIN" (one commentator memorably described DODIN as "really not a single network, but a quasi-feudal patchwork of often incompatible local networks[;] It's the Holy Roman Empire of cyberspace"). Note, though, that the military does not normally have the role of defending *other* networks, such as those of the civilian parts of government or of the private sector.

3. Operations to cause effects - The military also may conduct cyber operations to cause effects (which might include disruption or alteration of communications, alteration of data, or perhaps even damage to physical systems controlled by software). The most obvious setting in which this might occur would be armed conflict. But the military is capable, in theory, of engaging in such activity in circumstances that do not rise to the level of armed conflict. Should it do so? As we will read in just a moment, Congress thinks the answer is yes and recently passed legislation to encourage such operations in certain settings. **For now, the important thing is to appreciate that the military's role in conducting cyber operations for effect is not necessarily limited to circumstances of armed conflict.**

Of these three categories of cyber activity, both ISR and operations to cause effect are likely to involve unauthorized access to someone else's network or device.

B. A Caution About Terminology

Before we move on, a word of caution is in order. You no doubt appreciate that there can be a significant difference between the common usage of a term and the way that the same term might have a specific, technical meaning for specialized audiences like lawyers. This can produce mutual misunderstanding, and you should be particularly alert for this problem when someone is describing cyber activities.

The words "war" and "warfare" are good examples. Those words have much less legal significance today than they used to (today the critical international law concept is "armed conflict" rather than "war"). Still, they remain words with significant resonance, and people —including influencers like journalists and politicians—employ them routinely. This is unproblematic when the words are used in relation to the paradigm case of warfare, in which militaries use lethal force against one another. But beyond that paradigm scenario, disagreement begins to emerge regarding which other situations also warrant those same labels. The words prove to be both vague and ambiguous, especially when someone uses them in connection with cyber activities that are not simply part of a larger, conventional armed conflict. And yet the words often are used in precisely that setting. The word "attack" is much the same. It too is both vague and ambiguous, and it too is used promiscuously in describing cyber activities.

- Do a search to find recent news articles that use the words "cyberwar" or "cyber attack." **Do any of the examples seem misplaced?**
- **Is there any real harm from using the language of war and attack in expansive ways when describing cyber activities?**
- **If you think there is overuse and that the overuse is harmful, can you think of plausible alternative language?**

C. An Introduction to CYBERCOM

Our next task is to become acquainted with the institutional structures the U.S. military has adopted in order to facilitate its activities in cyberspace. As you might expect, there has been a great deal of organizational change in recent years, and more is likely to come in the near future. We will not attempt anything close to a comprehensive overview, but we will at least identify some of the most important current institutions and some of the bigger issues that they face.

As an initial matter, let's recall that the NSA itself is part of the Defense Department, and that one of its core missions has long been collection of signals intelligence (a form of ISR) for combat-support purposes. The Defense Department also has long had a centralized organization (known since the early 1990s as the Defense Information Systems Agency ("DISA")) to build, maintain, and (to some extent) defend military communication systems. The gradual emergence of cyberspace greatly complicated the organizational picture, however, especially as it began to become clear that cyberspace was not just a medium for communication but also an operational domain analogous to land, air, water, and space in that one can conduct operations for effect there.

As Fred Kaplan explains in his book *Dark Territory: The Secret History of Cyber War* (available here if you are interested in going deeper), the military's effort to reorganize for cyber operations traces back to the late 1990s. As the Department began to appreciate how vulnerable its own networks were, it established a new office (the "Joint Task Force—Computer Network Defense," or just "JTF-CND") to coordinate defensive efforts. Kaplan writes that the

> "initial plan was to give [JTF-CND] an *offensive* role as well, a mandate to develop options for attacking an adversary's network.... [But the organizer] knew that the services wouldn't grant such powers to a small bureau with no command authority. ... [Eventually, in] 2000, JTF-CND became JTF-CNO, the *O* standing for "Operations," and those operations included not just Computer Network Defense but also, explicitly, Computer Network *Attack*.... [JTF-CNO] was placed under the purview of U.S. Space Command...it was an odd place to be, but SpaceCom was the only unit that wanted the mission...[and] in any case, it was a *command*, invested with war-planning and war-fighting powers. [But key leaders] felt that the cyber missions—especially those dealing with cyber *offense*—should ultimately be brought to the Fort Meade headquarters of the NSA." (pp. 121-22)

It took many years, but that is what happened in the end. In the summer of 2009, Secretary of Defense Gates directed the creation of a new command—United States Cyber Command (CYBERCOM)—focused on both defensive and offensive functions. In order to ensure its rapid maturation, moreover, the new command would be collocated with NSA at Ft. Meade, and NSA's Director would be "dual-hatted" as the CYBERCOM commander as well. This would enable NSA to incubate CYBERCOM in terms of personnel, knowledge, technical capabilities, and so forth. Less obviously, it also would ensure a process for deconfliction of priorities should the interests of CYBERCOM in causing an operational effect in cyberspace come into conflict with the interests of NSA in collecting intelligence.

- **Can you hypothesize a situation in which NSA collection equities and CYBERCOM operational interests might conflict?**

So, what exactly is CYBERCOM's role? The Defense Department's 2015 Cyber Strategy document provides a handy explanation:

> *"In 2012, DoD began to build a [Cyber Mission Force ("CMF")] to carry out DoD's cyber missions. Once fully operational, the CMF will include nearly 6,200 military, civilian, and contractor support personnel from across the military departments and defense components.... The Cyber Mission Force will be comprised of cyber operators organized into 133 teams, primarily aligned as follows:*
>
> > ***Cyber Protection Forces** will augment traditional defensive measures and defend priority DoD networks and systems against priority threats;*
> >
> > ***National Mission Forces** and their associated support teams will defend the United States and its interests against cyberattacks of significant consequence; and*
> >
> > ***Combat Mission Forces** and their associated support teams will support combatant commands by generating integrated cyberspace effects in support of operational plans and contingency operations.*
>
> *Combatant commands integrate Combat Mission Forces and Cyber Protection Teams into plans and operations and employ them in cyberspace, while the National Mission Force operates under the Commander of USCYBERCOM. Outside of this construct, teams can also be used to support other missions as required by the Department."*

Put simply, CYBERCOM has three core missions: defend DODIN (that's the job of the Cyber Protection Forces); provide combat support (that's the job of the Combat Mission Forces); and in special circumstances defend the nation more generally (that's the job of the National Mission Forces).

Note the reference above to "combatant commands," which will employ the Combat Mission Forces and to some extent the Cyber Protection Forces as well. This calls for a quick primer on what a "combatant command" is and how CYBERCOM fits into that picture.

The traditional organizational structure of the Armed Forces of the United States involved a sharp division into a series of separate "service branches": the Army, Navy, Air Force, and Marines (and the Coast Guard as well, though its precise status is complicated). The several branches not only recruited, trained, and equipped their own forces, but in the past they also planned and commanded their own operations (often, though not always, in coordination with one another). Today, they continue to recruit, train, and equip separately, but they no longer plan and command operations independently. We now have a "joint forces" model for purposes of actual operations. Under this model, assets generated by each branch come under the operational control of a single, unified command structure. More specifically, we now have a globe-spanning series of geographically-defined "combatant commands," such as Central Command (CENTCOM, which encompasses the Middle East through to Afghanistan) and Indo-Pacific Command (INDOPACOM).

So far so good, but it gets more complicated. In addition to these geographically-defined commands, we also have several additional commands that have no geographic boundaries but instead are defined by the particular functions they perform or support. CYBERCOM is such a command. Special Operations Command (SOCOM) is another. These functional

commands are like the geographic ones in that their subordinate units and personnel are mostly generated by the various service branches, but then brought together under a "joint" command structure for operational purposes. In CYBERCOM's case, that means that Army, Navy, Air Force, and Marine units and personnel make up the various Cyber Mission Forces.

Against that backdrop, it is easier to understand the description of CYBERCOM's various missions. First, CYBERCOM is charged with ensuring that the geographic combatant commands like CENTCOM are supported with both Combat Mission Forces and Cyber Protection Teams. Second, more generally, CYBERCOM oversees the defense of DODIN. Third, and most intriguingly, CYBERCOM has its own, direct operational responsibility in those limited circumstances in which it is ordered to defend the nation against significant cyber activities (this is the role of the National Mission Forces).

Notice how that last role might dovetail with the issue we raised at the outset of this reading, regarding the role of the military in conducting cyber operations for effect outside the context of armed conflict. We'll talk more about that below. But first, consider this question:

- You likely have heard that President Trump has called for the creation of Space Force as a new service branch in the U.S. military. **Should we instead (or in addition) create Cyber Force, such that the task of recruiting, training, and equipping cyber mission teams falls to an independent branch rather than Army, Navy, Air Force, and Marines?**

D. Unleashing CYBERCOM for Combat-Related Operations?

As CYBERCOM has matured, questions have arisen about whether it should move more aggressively to cause operational effects. For example, such questions have arisen in relation to combat operations. The following text is excerpted from a post I wrote for *Lawfare* in 2017, detailing problems that emerged when the Defense Department wanted CYBERCOM to conduct certain operations in relation to the armed conflict with the Islamic State:

> **1. July 2016 – Reports of DOD frustration over pace of anti-ISIS cyber operations**
>
> In July 2016, the Washington Post (Ellen Nakashima & Missy Ryan) reported on CYBERCOM's efforts to disrupt the Islamic State's online activities (internal communications, external propaganda, financing, etc.), emphasizing the view of DOD leadership that CYBERCOM was underperforming:
>
> > *An unprecedented Pentagon cyber-offensive against the Islamic State has gotten off to a slow start, officials said, frustrating Pentagon leaders and threatening to undermine efforts to counter the militant group's sophisticated use of technology for recruiting, operations and propaganda. …*
> >
> > *But defense officials said the command is still working to put the right staff in place and has not yet developed a full suite of malware and other tools tailored to attack an adversary dramatically different from the nation-states Cybercom was created to fight. …*

> *Although officials declined to detail current operations, they said that cyberattacks occurring under the new task force might, for instance, disrupt a payment system, identify a communications platform used by Islamic State members and knock it out, or bring down Dabiq, the Islamic State's online magazine. …*

The report is an excellent snapshot of several distinct challenges the military use of computer network operations can pose.

One such challenge is **operational capacity.** The story suggests that CYBERCOM simply did not have the right personnel and the right exploits on hand for this particular mission, at least at the start. That's a problem that can be fixed, and the report details the steps DOD began taking in 2016 to do just that.

Another challenge is the need to have an effective process for **deconfliction between intelligence-collection and operational-effect equities.** As the article summarized the issue:

> *Whenever the military undertakes a cyber-operation to disrupt a network, the intelligence community may risk losing an opportunity to monitor communications on that network. So military cybersecurity officials have worked to better coordinate their target selection and operations with intelligence officials.*

This is not a novel tension, in the abstract. For as long as there has been signals intelligence, there have been tensions of this kind. When one side has access to the other's communications, there will always be tension between the temptation to exploit that access for operational effect (with the opportunity cost of risking loss of that access going forward as the enemy realizes it has been monitored) and the temptation to instead exploit it for indirect intelligence advantage (with the opportunity cost of forgoing direct operational advantage in at least some cases). World War II provides famous examples. And so one might fairly ask: is there anything really different about computer network operations, warranting special attention to the topic in this setting?

Perhaps. In this domain there is much more overlap between the means of collection and the means of carrying out a disruptive operations. Indeed, those means often will be the exact same: a particular exploit providing access to an enemy device, network, etc. It seems to me that this ensures that the tension between collection and operational equities will arise with greater frequency, and less room for workarounds, than in more familiar settings.

Having mentioned both the operational capacity concern and the competing-equities concern, now is a good time to emphasize the significance of the status-quo for NSA and CYBERCOM: the dual-hatted commander. Whereas more familiar, traditional scenarios involving tension between collection and operational equities usually involve distinct underlying institutions and commanders, the status quo with respect to computer network operations has always (well, the past seven years) involved the dual-hatting of NSA's director and CYBERCOM's commander.

This model in theory ensures that neither institution has a home-field advantage, and maximizes the chance that the key decisionmaker (yes, there can be important decisions both below and above the dual-hat, but the dual-hat is obviously in the key position) fully buys into and fully grasps the importance of each institution's mission.

Of course, it is possible that the dual-hat might tilt one direction to an unfair or undesirable degree. And it is possible that some might perceive such a tilt even when there isn't one. As 2016 wore on, questions of this kind began to appear in public, and by September the media was reporting that DNI Clapper and SecDef Carter both were in favor of splitting up the dual-hat. It was not the first time this topic had come up, to be sure; President Obama had considered ordering a split in 2013 (during the aftermath of the Snowden controversy), but had not taken that step at least in part out of concern about CYBERCOM's independent operational capacity. Now the idea appeared to have momentum.

A report from Ellen Nakashima in the Washington Post that same month suggested that this momentum was in part a product of CYBERCOM's operational maturation, but also in significant part driven by the perception that Admiral Rogers, the current dual-hat, favored collection equities to an undue extent:

> *"Whether or not it's true, the perception with Secretary Carter and [top aides] has become that the intelligence agency has been winning out at the expense of [cyber] war efforts," said one senior military official….*

(See also this report by the New York Times, stating that frustration along these same lines contributed to the effort to get President Obama to remove Admiral Rogers in late 2016.)

The Washington Post report also highlighted concerns that splitting NSA and CYBERCOM at the leadership level might actually weaken rather than empower CYBERCOM, as NSA inevitably would become free to withhold from CYBERCOM at least some exploits or other forms of access so that sources would not be lost:

> *"Cyber Command's mission, their primary focus, is to degrade or destroy," the former official said. "NSA's is exploit [to gather intelligence] only. So without having one person as the leader for both, the bureaucratic walls will go up and you'll find NSA not cooperating with Cyber Command to give them the information they'll need to be successful."*

2. December 2016 – Congress puts on the brakes

Against this backdrop, Congress intervened in late 2016 to slow down the Obama administration's move to split the dual-hat. Section 1642 of the NDAA FY'17, enacted in late December, provides that NSA and CYBERCOM must continue to share a dual-hatted director/commander unless and until the Secretary of Defense and the Chairman of the Joint Chiefs of Staff jointly certify to certain Congressional committees (SASC & HASC; SSCI & HPSCI; and the Appropriations Committees) that separation will not pose "unacceptable" risks to CYBERCOM's effectiveness, and that the following six conditions are met:

> *(i) Robust operational infrastructure has been deployed that is sufficient to meet the unique cyber mission needs of the United States Cyber Command and the National Security Agency, respectively.*
>
> ***(ii) Robust command and control systems and processes have been established*** *for planning,* ***deconflicting****, and executing* ***military cyber operations****.*
>
> *(iii) The tools and weapons used in cyber operations are sufficient for achieving required effects.*

> *(iv) Capabilities have been established to enable intelligence collection and operational preparation of the environment for cyber operations.*
>
> *(v) Capabilities have been established to train cyber operations personnel, test cyber capabilities, and rehearse cyber missions.*
>
> *(vi) The cyber mission force has achieved **full operational capability**.*

Section 1642(b)(2)(C) (emphasis added). President Obama's signing statement criticized Congress for imposing this requirement, but did not include a claim that it was unconstitutional. It remains the law at this time.

3. Early 2017 – Complications in the War Against the Islamic State

While lawmakers and policymakers wrestled with the pros and cons of splitting NSA and CYBERCOM, computer network operations against the Islamic State continued to accelerate.

Along the way, however, new problems emerged.

As Ellen Nakashima of the Washington Post reported in May 2017, CYBERCOM by late 2016 had encountered a new set of challenges in its enhanced effort to shut down ISIS sites and platforms: **third-country effects.**

> *"A secret global operation by the Pentagon late last year to sabotage the Islamic State's online videos and propaganda sparked fierce debate inside the government over whether it was necessary to notify countries that are home to computer hosting services used by the extremist group, including U.S. allies in Europe. … Cybercom developed the campaign under pressure from then-Defense Secretary Ashton B. Carter, who wanted the command to raise its game against the Islamic State. But when the CIA, State Department and FBI got wind of the plan to conduct operations inside the borders of other countries without telling them, officials at the agencies immediately became concerned that the campaign could undermine cooperation with those countries on law enforcement, intelligence and counterterrorism. The issue took the Obama National Security Council weeks to address…"*

This article highlights a third significant challenge associated with computer network operations: attacking the enemy's online presence often requires, or at least risks, some degree of impact on servers located in other countries. Third-country impact involves both legal and policy challenges, and as the quote above illustrates it also brings into play otherwise-unrelated equities of other agencies. Thus, the competing-equities tension is not just a clash between collection and operational equities, but in some cases many others as well. The dual-hat command structure is primarily an answer only to the former, not the latter.

Meanwhile, a sobering reality about the utility of cyberattacks on Islamic State communications began to become clear: the effects often did not last. This was the thrust of an important piece by David Sanger and Eric Schmitt in the New York Times in June 2017:

> *[S]ince they began training their arsenal of cyberweapons on …internet use by the Islamic State, the results have been a consistent disappointment, American officials say. … [It] has become clear that recruitment efforts and communications hubs reappear almost as quickly as they are torn down. …*

> *"In general, there was some sense of disappointment in the overall ability for cyberoperations to land a major blow against ISIS," or the Islamic State, said Joshua Geltzer, who was the senior director for counterterrorism at the National Security Council until March. "This is just much harder in practice than people think..."*

This suggested that the military equities that some felt had been undervalued by Admiral Rogers in the past were less weighty than proponents had assumed. Nonetheless, momentum towards separation—and concern that the dual-hat unduly favors collection equities—continues.

In mid-July, reports emerged that the Pentagon had submitted to the Trump administration a plan for effectuating the split, with some of the accompanying commentary continuing to advance the argument that NSA holds CYBERCOM back to an improper extent:

The goal, [unnamed U.S. officials] said, is to give U.S. Cyber Command more autonomy, freeing it from any constraints that stem from working alongside the NSA, which is responsible for monitoring and collecting telephone, internet and other intelligence data from around the world — a responsibility that can sometimes clash with military operations against enemy forces.

This account raises a number of questions for you to consider:

- **Can you list the variables that may have constrained CYBERCOM in conducting operations for effect against the Islamic State?**
- **What are the pros and cons of ending the dual-hat arrangement?**
- Military operations that produce damage in the physical world often are followed by enemy efforts to repair that damage and restore functionality. **Is there reason to think such remediation efforts are, on the whole, easier in cyberspace?**

The account above refers to interagency battles over potential CYBERCOM operations, with CIA, State, and Justice objecting at certain points. This might cause you to wonder: What put those organizations in a position even to know about those plans, let alone to object effectively at the White House level? The answer has to do with an Obama administration policy directive that reportedly required interagency vetting of this sort for military cyber operations expected to have effects outside of areas of active hostilities. Notably, Trump administration officials have announced that this requirement has been revoked (in the form National Security Presidential Memorandum 13, the precise details of which are not yet public).

- **What are the pros and cons of removing the interagency vetting requirement?**

E. Unleashing CYBERCOM for Operations Below the Threshold of Armed Conflict?

Questions also have arisen about the authority of CYBERCOM (and especially the National Mission Forces, as noted above) to engage in operations to defend the nation against significant cyber activities outside the context of armed conflict. For example, can and should the National Mission Forces be used to conduct operations outside of DODIN—and

perhaps even outside the United States—in response to efforts by foreign governments or other entities to use cyber means to interfere with U.S. elections?

Congress thinks the answer should be yes, and took steps in the most-recent National Defense Authorization Act to prune away certain potential obstacles to an active CYBERCOM role. In particular, it sought to make clear both that (1) CYBERCOM has affirmative authority to engage in such activity in certain contexts and (2) CYBERCOM actions under that authority must be categorized as "TMA" rather than "covert action." Let's have a look at the new statutory language on these points, and then answer some questions

First, Section 1642 of the NDAA Fiscal Year '19 provides in relevant part that:

> **(a) AUTHORITY TO DISRUPT, DEFEAT, AND DETER CYBER ATTACKS.—**
>
> **(1) IN GENERAL.—**In the event that the National Command Authority determines that the Russian Federation, People's Republic of China, Democratic People's Republic of Korea, or Islamic Republic of Iran is conducting an active, systematic, and ongoing campaign of attacks against the Government or people of the United States in cyberspace, including attempting to influence American elections and democratic political processes, the National Command Authority may authorize the Secretary of Defense, acting through the Commander of the United States Cyber Command, to take appropriate and proportional action in foreign cyberspace to disrupt, defeat, and deter such attacks under the authority and policy of the Secretary of Defense to conduct cyber operations and information operations as traditional military activities.

Consider these questions about that provision:

- **What conditions must be met in order for this grant of authority to come into play?**
- **Does anything go once the authority comes into play?**
- **Can you relate this authority to the decision by the Trump administration to revoke interagency vetting of military cyber operations expected to have effects outside of combat zones?**

Second, Section 1632 of the NDAA provides that "clandestine military activity or operation in cyberspace shall be considered a traditional military activity," full stop.

- **What is the practical effect of compelling the conclusion that "clandestine" military activity in cyberspace counts as TMA?** Go back and review the discussion of TMA and covert action in the prior reading if needed.

Note, though, that other statutory provisions require DOD to report to Congress (specifically, the Senate and House Armed Services Committees) on certain cyber activities. For example, 10 USC 130j is a 2017 law that requires the Secretary of Defense to issue a written notice to the House and Senate Armed Services Committees within 48 hours for "sensitive military cyber operations," defined to encompass any military cyber operation intended to have an effect overseas in a location that is not itself a combat zone."

- **Why be concerned to ensure oversight in that scenario?**

- **Why exclude situations in which the effect is expected in a combat zone?**

Separately, 10 USC 484 requires the Secretary of Defense to provide quarterly briefings to the Armed Services Committees on "offensive and significant defensive military operations in cyberspace" without reference to where those operations were intended to have an effect.

- **Can you explain how the Section 484 reporting requirement differs from Section 130j?**

F. Defending Forward?

An unclassified summary of the 2018 Defense Department Cyber Strategy made waves recently, thanks to this passage:

> *"We will conduct cyberspace operations to collect intelligence and prepare military cyber capabilities to be used in the event of crisis or conflict. We will defend forward to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict."*

- **Can you relate the idea of "defending forward" to any of the authorities described above?**
- Notice the separate reference to "prepare military cyber capabilities to be used in the event of crisis or conflict". **Can you relate this to our prior discussions of "preparation of the battlefield" and "hold at risk"?**

24. December 5 Cyber War? International Law Concerns

Over the past two classes, we examined situations in which both intelligence agencies and the U.S. military might engage in unauthorized access of foreign networks and systems. We've looked at many provisions of U.S. law under that heading, but have not yet looked at what international law might have to say about it. In this final substantive session, we will focus exclusively on that question.

A. International Law: A Brief Backgrounder

Some of you will be familiar already with the nature of international law, but for the benefit of the rest I will provide a brief overview here.
First, please note that when we speak of "international law" we are *not* talking about the law of any one particular foreign country. The law of Russia is simply "foreign law" from a U.S. perspective, just as America's law is merely foreign law from a Russian perspective. International law, in contrast, by definition exists on the international plane.

The traditional understanding is that international law can come into being in two ways. First, sovereigns can form agreements—treaties—pursuant to which they voluntarily embrace certain obligations or constraints. This has the advantage of relative clarity, but note that it binds only the parties to the treaty. Second, international law also can come into existence via "custom" (i.e., "customary international law"), so long as two conditions are met: there must be a common, settled usage or practice undertaken or complied with by states, and they must do this out of a sense of legal obligation (and, yes, that is more than a bit circular in its logic). Customary international law thus is less determinate than a treaty, to put it mildly, but on the other hand it is thought to be binding (at least on the

international plane) on all states (excepting those that persistently and expressly object to an emerging customary rule).

As you might expect, some are relatively strict while others are relatively flexible in making a judgment about whether a rule of customary international law has come into being. Relatedly, some are more willing than others to give evidentiary weight to statements by government officials that are not directly connected to actual actions by their state. And some are more willing than others to point to statements by courts, international bodies, and academics. In short, there is much friction over the mechanics of determining customary international law, not to mention arguments about which potential rules properly make the cut.

This point helps to contextualize a concept that comes up often in the cyber context: the idea of international "norms." To say that something is a "norm" is *not* the same thing as saying that it is an established rule of customary international law, let alone a rule embedded in a treaty. It is no more and no less than a claim that some grouping has endorsed the desirability of acting or not acting in a certain way. If the grouping consists of states and is numerous—and if the actual activities of those states is consistent with their stated normative preference—then this can go some way towards an argument for recognition of a rule of customary international law. But be wary that those conditions really are met before assuming that an asserted "norm" is on its way towards having legal force; always consider who has asserted the norm, whether the state practice actually conforms to it, and whether it can fairly be said to have achieved the uniformity of compliance and sense of legal obligation that is supposed to characterize actual customary international law.

B. International Law & International Relations

Before digging into the content of existing international law that might relate to cyber operations across borders, we might pause to consider whether and why a government would care in practical terms about such constraints (and whether all governments are likely to care equally).

- **Create a list of practical reasons the U.S. government might be wise to care.**
- **For each item on your list, consider whether that reason applies with the same force for China.**

C. Cyber Operations and the United Nations Charter

There is no multilateral treaty *expressly* restricting how states might use cyber operations against one another's interests. Any treaty-based constraints on cyber activities must instead be based on some other, more-general, treaty. And that brings us to the Charter of the United Nations. The Charter contains a number of rules that are important to cross-border cyber activity.

1. Use of Force

Most notably, Article 2(4) of the U.N. Charter creates a default rule prohibiting the "use of force" in international affairs. This rule carries with it legal, diplomatic, and political consequences. Most notably: the U.N. Security Council (consisting of five permanent members (the United States, the United Kingdom, France, China, and Russia) as well as a rotating cast of other states) determines that a state has violated this rule, it may authorize an array of significant responses (including economic sanctions and, in the most extreme cases, approval for other states themselves to use force in order to restore international peace).

- Ponder the various types of cyber activity we have considered in this course. **Can you think of some that, considered in isolation, might qualify as "force"?**

Notwithstanding this rule, an action that counts as a "use of force" is not prohibited by Article 2(4) in at least three circumstances:

> **Consent:** An otherwise-forbidden use of force impacting another state is permitted if the that state consents to it.
>
> **Security Council Authorization:** As noted above, the U.N. Security Council has authority to issue authorizations to member states to use force in limited circumstances.
>
> **Self-Defense:** Article 51 of the U.N. Charter provides that states may use force in self-defense (as well as defense of another state, if requested by that state) in the event of an "armed attack." Note that there is fierce debate about whether and to what extent Article 51 self-defense includes situations in which the armed attack is merely anticipated but has not yet occurred. There also is considerable debate about whether the threshold to count as an "armed attack" triggering this right of self-defense should be higher than the threshold for "use of force," with the U.S. taking the position that there is no gap but others disputing the point. At any rate, if and when self-defense rights are properly invoked, the defending state must limit its responsive use of force to means that are both "necessary" and "proportional" to the provocation.

Some states—including the United States—take the view that there is a fourth scenario in which an otherwise-forbidden use of force is permissible:

> **Unwilling/Unable:** On this view, a "host state" that is unable or unwilling to prevent or suppress a non-state actor within its territory from engaging in armed attacks on other states cannot complain under Article 2(4) if the victim state (or a state the victim asks to come to its aid) uses necessary and proportionate force In the host state's territory against the attacker. This is a controversial position that first gained attention when invoked by the United States in relation to drone strikes against al Qaeda and related targets, and then gained wider acceptance when used by the United States and others to explain how it was lawful to use force against Islamic State targets in Syria even without permission of the Assad regime.

In light of this framework, consider the following questions:

- **Can you explain why it might prove difficult to apply the Article 51 rule in the cyber context?** Note: the Tallinn Manual 2.0 (more about it below) argues that a "cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force."
- **Can you explain why it also might prove difficult to apply the unwilling/unable test?**
- **From the point of view of the victim state (and its allies), should it matter whether the state that engaged in the cyber operation:**

  > **(1) used military forces, an intelligence agency, a private contractor, or any other institutional means to conduct the activity?**
  >
  > **(2) acknowledges that it conducted the activity?**

2. Internationally Wrongful Acts and Countermeasures

Just because a cyber action falls shy of the "use of force" standard does not mean that international law has nothing to say about it. The action might still violate some other rule of international law apart from Article 2(4), and that in turn might open the door to responsive "countermeasures" by the victim state.

To understand these concepts better, let's refer to the "Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations." The Tallinn Manual is not itself a legal instrument, though it is written in terms of "rules." It is a scholarly product, resulting from a multi-year set of discussions among a large group of international law experts from a variety of countries (conducted under the auspices of the NATO Cooperative Cyber Defense Center of Excellence, but not constituting the views of NATO or any particular state as such). It is framed as a summary of current law accompanied by commentaries (though some critics contend that some of the rules it identifies are more aspirational than descriptive of existing law). It is, at any rate, far-and-away the most influential attempt thusfar to describe how existing international law rules apply to various cyber scenarios, not to mention a convenient way to frame our discussion.

Rule 20 of the manual provides that a "State may be entitled to take countermeasures, whether cyber in nature or not, in response to a breach of an international legal obligation that it is owed by another State." Put more directly: if one state acts illegally towards another, it opens up the door to the victim retaliating with methods that otherwise would violate international law.

Countermeasures are not punitive as such. Rather, they must be intended to induce the offending state to stop violating international law. (Rule 21) They are not an anything-goes situation, either. They may not "affect fundamental human rights," for example. (Rule 22) And they "must be proportionate to the injury to which they respond." (Rule 23) They need not involve the same means or domain that produced the original injury, however; they can be cross-domain in nature. (Rule 24)

- Assume that a Russian intelligence agency is in the midst of conducting a covert action program to influence an American election. **Can you identify a countermeasure the United States might then employ that is both compliant with the aforementioned constraints and might actually have an impact?**
- Same situation, but the election is now over. You are told that there is good reason to believe the same thing will happen in the next election, though there is no intelligence thusfar confirming that such an operation already is underway. **Is the option of countermeasures currently available?**

Countermeasures by definition come into play only where the other state has engaged in a wrongful act (or where that state is responsible for the wrongful acts of private individuals/entities who did so). This raises the question of what wrongful facts, other than the "use of force" situation under Article 2(4) of the UN Charter, would trigger the countermeasure option.

Here, there is considerable debate, particularly as applied to cyber operations. The key thing to grasp is that the debate revolves around the concept of "sovereignty," and is expressed in terms of differing view about what customary international law has to say about protection of sovereignty in contexts below the threshold of the use of force. For the most part, there is agreement that conduct constituting "coercive intervention" in a sovereign's affairs is covered. Precisely what counts as coercive intervention is contested, however, and beyond that there also is debate about whether non-coercive intrusions into

sovereignty also might be treated as prohibited as a matter of customary international law (notice how this latter point might resonate for governments that hold to a strong view of sovereign prerogative in non-cyber settings).

Here is an excerpt from a much-noticed articulation of the British view of these questions, from then Attorney General Jeremy Wright in May 2018:

> "In certain circumstances, cyber operations which do not meet the threshold of the use of force but are undertaken by one state against the territory of another state without that state's consent will be considered a breach of international law.
>
> The international law prohibition on intervention in the internal affairs of other states is of particular importance in modern times when technology has an increasing role to play in every facet of our lives, including political campaigns and the conduct of elections. As set out by the International Court of Justice in its judgment in the Nicaragua case, the purpose of this principle is to ensure that all states remain free from external, coercive intervention in the matters of government which are at the heart of a state's sovereignty, such as the freedom to choose its own political, social, economic and cultural system.
> The precise boundaries of this principle are the subject of ongoing debate between states, and not just in the context of cyber space. But the practical application of the principle in this context would be the use by a hostile state of cyber operations to manipulate the electoral system to alter the results of an election in another state, intervention in the fundamental operation of Parliament, or in the stability of our financial system. Such acts must surely be a breach of the prohibition on intervention in the domestic affairs of states.
>
> Furthermore, a breach of this principle of non-intervention provides victim states with the ability to take action in response that would otherwise be considered unlawful, but which is permissible if it is aimed at returning relations between the hostile state and the victim state to one of lawfulness, and bringing an end to the prior unlawful act. Such action is permissible under the international law doctrine of countermeasures. Put simply, if a hostile state breaches international law as a result of its coercive actions against the target state's sovereign freedoms, then the victim state can take action to compel that hostile state to stop.
>
> Consistent with the de-escalatory nature of international law, there are clear restrictions on the actions that a victim state can take under the doctrine of countermeasures. A countermeasure can only be taken in response to a prior internationally wrongful act committed by a state, and must only be directed towards that state. This means that the victim state must be confident in its attribution of that act to a hostile state before it takes action in response. In cyberspace of course, attribution presents particular challenges, to which I will come in a few moments. Countermeasures cannot involve the use of force, and they must be both necessary and proportionate to the purpose of inducing the hostile state to comply with its obligations under international law.
>
> These restrictions under the doctrine of countermeasures are generally accepted across the international law community. The one area where the UK departs from the excellent work of the International Law Commission on this issue is where the UK is responding to covert cyber intrusion with countermeasures.
>
> In such circumstances, we would not agree that we are always legally obliged to give prior notification to the hostile state before taking countermeasures against it. The covertness and secrecy of the countermeasures must of course be considered

> necessary and proportionate to the original illegality, but we say it could not be right for international law to require a countermeasure to expose highly sensitive capabilities in defending the country in the cyber arena, as in any other arena.
>
> In addition, it is also worth stating that, as a matter of law, there is no requirement in the doctrine of countermeasures for a response to be symmetrical to the underlying unlawful act. What matters is necessity and proportionality, which means that the UK could respond to a cyber intrusion through non-cyber means, and vice versa.
>
> Through the principle of non-intervention, it is clear that the international community has set a boundary at which interference in another state's sovereign freedoms is considered internationally wrongful and as such, in breach of international law, giving rise to the right to take action which may otherwise be unlawful in response. As I have already mentioned, the precise parameters of this principle remain the subject of ongoing debate in the international law community, but a further contested area amongst those engaged in the application of international law to cyber space is the regulation of activities that fall below the threshold of a prohibited intervention, but nonetheless may be perceived as affecting the territorial sovereignty of another state without that state's prior consent.
>
> Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent.
>
> Sovereignty is of course fundamental to the international rules-based system. But I am not persuaded that we can currently extrapolate from that general principle a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention. The UK Government's position is therefore that there is no such rule as a matter of current international law."

It is widely thought that this reflects the U.S. position as well. Here is language from a speech by Brian Egan, then the Legal Adviser of the State Department, in 2016:

> "In certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law, even if it falls below the threshold of a use of force. This is a challenging area of the law that raises difficult questions. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States.
>
> Relatedly, consider the challenges we face in clarifying the international law prohibition on unlawful intervention. As articulated by the International Court of Justice (ICJ) in its judgment on the merits in the Nicaragua Case, this rule of customary international law forbids States from engaging in coercive action that bears on a matter that each State is entitled, by the principle of State sovereignty, to decide freely, such as the choice of a political, economic, social, and cultural system. This is generally viewed as a relatively narrow rule of customary international law, but States' cyber activities could run afoul of this prohibition. For example, a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention. For increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States' activities in cyberspace.

In light of Egan's reference to states collaborating to clarify how international law applies in this setting, it is worth noting that the UN for many years has sponsored a "Group of Government Experts" ("GGE") process focused on identifying points of agreement on such matters. In 2017, the most recent round of this process collapsed in the face of the unwillingness of some states (Cuba, most conspicuously, but with support from Russia and China) to agree that various bodies of international law (such as the laws of armed conflict) even apply in the cyber context.

- **Can you explain how the varying national interests and circumstances of the United States, Russia, and China might cause them to take different positions in the context of such negotiations?**

Notably, Egan asserted in that same 2016 speech that espionage does not qualify as a violation of international law (though of course it almost always violates the domestic law of the foreign state that is the subject of the collection). So too the Tallinn Manual 2.0 at Rule 32, though the manual observes that the answer might be different depending on the collateral consequences of the espionage.

- **Can you explain how this complicates the legal analysis for a victim state that has detected an intrusion and attributed it to a foreign government, in circumstances where the system penetrated contains useful information and also performs important functions?**

A final wrinkle: Tallinn Manual 2.0 also asserts, at Rule 26, that a "State may act pursuant to the plea of necessity in response to acts that present a grave and imminent peril, whether cyber in nature or not, to an essential interest when doing so is the sole means of safeguarding it."

Let's now apply some of these concepts:

- Assume that the United States and Israel have combined forces to create malware that will cause physical damage to centrifuges in an Iranian nuclear facility. **Does this constitute an armed attack? A use of force? A coercive intervention?**
- Assume the answer is that it appears at first blush to have been a coercive intervention. **Could the U.S. and Israel make an argument that it was, in fact, a countermeasure?**
- **What considerations, apart from legal ones, might impact the manner in which Iran chooses to categorize the activity once it learns of it?**
- **Imagine that CYBERCOM manages to hack into a Russian military communications system, and steals data from it. Is that a "use of force"? "Armed attack"? "Coercive intervention"?**
- **Same questions, but this time CYBERCOM causes the system to stop functioning for one hour.**
- **Same, but this time CYBERCOM causes the system to overheat, resulting in physical damage that ruins the system.**
- **Same, but this time CYBERCOM causes the system to explode, killing several nearby personnel.**

D. Cyber Operations During Armed Conflict

Does the law of armed conflict apply to computer network operations? That is, are they subject to the familiar law of armed conflict rule such as the prohibition on intentionally attacking civilians and civilian objects (a rule that has exceptions, of course, such as the exception for civilians who are in the midst of participating in hostilities, or civilian objects being used for military purposes), and the "collateral damage" rule that forbids attacks on otherwise-permissible targets where the anticipated civilian harm will outweigh the expected military benefit. The Tallinn Manual 2.0 explains the majority view (which the United States and its allies share):

> **Rule 80: "Cyber operations executed in the context of an armed conflict are subject to the law of armed conflict."**
>
> *Does it mean that all computer network operations conducted by a military entity are subject to the law of armed conflict at all times? Conversely, does it mean that computer network operations conducted by a non-military unit are not so subject?*

E. Cyber Operations and Human Rights Law

A full treatment of this topic is beyond our scope, but for now it suffices to say that there is fierce disagreement regarding the extent to which the international human right to privacy (memorialized, for example, in Article 17 of the International Covenant on Civil and Political Rights, which forbids "arbitrary or unlawful interference with … privacy") is implicated by a foreign government's cyber activities conducted for purposes of espionage.

III. CRISIS SIMULATION

25. December 6 – Crisis Simulation

With Units I and II under our belts, the stage is set to integrate our accumulated knowledge in a practical setting. In the final class meeting we will conduct a crisis simulation exercise—a role-play simulating an unfolding cybersecurity crisis—that will give you a unique opportunity to work in teams to demonstrate, and practice with, what you have learned. There is no additional reading for this session.

IV. FINAL EXAM

December 14 – Good luck!